

Kerio Personal Firewall 4™

Uživatelský manuál

Kerio Technologies

© 1997-2003 Kerio Technologies. Všechna práva vyhrazena.

Datum vydání: 18. srpna 2003

Aktuální verze produktu: *Kerio Personal Firewall 4.0.0*. Změny vyhrazeny.

Obsah

1	Úvod	5
1.1	Kerio Personal Firewall 4.0	5
1.2	Plná a volně šiřitelná verze	7
1.3	Systémové požadavky	7
1.4	Konfliktní software	8
1.5	Instalace, upgrade a odinstalování	8
1.6	Kontrola nových verzí	9
1.7	Počáteční konfigurace	11
2	Komponenty firewallu a základní ovládání	13
2.1	Komponenty aplikace Kerio Personal Firewall	13
2.2	Ikona na nástrojové liště	14
2.3	Registrace produktu	16
3	Chování firewallu a interakce s uživatelem	21
3.1	Chování firewallu	21
3.2	Dialog Connection Alert (zachycení neznámé komunikace)	21
3.3	Dialog Starting/Replacing/Launching other application	25
3.4	Okno Alert (upozornění na událost)	28
4	Konfigurace firewallu	31
4.1	Konfigurační okno	31
4.2	Preference	33
4.3	Pravidla firewallu	36
5	Pravidla pro síťovou komunikaci	37
5.1	Pravidla pro aplikace	37
5.2	Předdefinovaná pravidla pro síťovou komunikaci	41
5.3	Definice důvěryhodné zóny	43
5.4	Rozšířený paketový filtr	44
6	Kontrola spouštěných aplikací (bezpečnost systému)	57
6.1	Pravidla pro aplikace	57
6.2	Obecná pravidla	59

7	Detekce útoků	61
7.1	Nastavení systému detekce útoků	61
8	Filtrování obsahu WWW stránek	65
8.1	Blokování reklam, skriptů a pop-up oken	65
8.2	Ochrana soukromí uživatele	68
8.3	Výjimky pro jednotlivé WWW servery	69
9	Stavové informace	73
9.1	Přehled spojení a otevřených portů	73
9.2	Statistiky	74
10	Záznamy	77
10.1	Prohlížení záznamů	77
10.2	Kontextové menu pro záznamy	78
10.3	Volby pro záznamy	79
10.4	Záznam Network	80
10.5	Záznam System	81
10.6	Záznam Intrusions	82
10.7	Záznam Web	83
10.8	Záznamy Debug, Error a Warning	84
11	Slovníček pojmů	85

1.1 Kerio Personal Firewall 4.0

Kerio Personal Firewall je aplikace určená k ochraně osobního počítače před útoky ze sítě (typicky z Internetu), viry a únikem dat. Tyto bezpečnostní funkce zajišťují čtyři hlavní moduly:

Network Security Tento modul sleduje veškerou síťovou (resp. TCP/IP) komunikaci počítače, na kterém je *Kerio Personal Firewall* nainstalován. Pro síťovou komunikaci může uživatel definovat dva typy pravidel:

- pravidla pro aplikace — pro každou aplikaci lze povolit nebo zakázat síťovou komunikaci, případně nastavit, aby se *Kerio Personal Firewall* dotázal uživatele.
- pravidla paketového filtru — zkušenější uživatelé mohou definovat detailní pravidla pro síťovou komunikaci (specifikace IP adres, protokolů, portů atd.). Tato pravidla mohou platit pro konkrétní aplikaci nebo obecně (pro libovolnou aplikaci).

Kerio Personal Firewall obsahuje také sadu předdefinovaných pravidel pro síťovou komunikaci (např. pro DNS, DHCP apod.). Tato pravidla jsou oddělená od uživatelsky definovaných pravidel a lze je jednoduše aktivovat či vyřadit.

Jestliže *Kerio Personal Firewall* zachytí komunikaci, pro kterou neexistuje odpovídající pravidlo, dotáže se uživatele, zda tuto komunikaci povolí či zakáže. Na základě odpovědi uživatele může být automaticky vytvořeno pravidlo pro aplikaci nebo pravidlo paketového filtru.

System Security Modul *System Security* kontroluje spouštění aplikací v operačním systému. Sledovány jsou tři typy událostí:

- spuštění aplikace
- změna ve spustitelném souboru aplikace od posledního spuštění (záměna aplikace)
- spuštění jiné aplikace běžící aplikací

Kapitola 1 Úvod

Podobně jako v případě síťové komunikace lze definovat pravidla pro jednotlivé aplikace, která příslušnou akci povolují nebo zakazují, případně vyžadují reakci uživatele. Pokud neexistuje odpovídající pravidlo, *Kerio Personal Firewall* se dotáže uživatele, zda spuštění aplikace povolí či zakáže.

Poznámka: *Kerio Personal Firewall 4.0* (narozdíl od starších verzí) kontroluje spuštění všech aplikací, bez ohledu na to, zda se účastní síťové komunikace. V případě infekce virem reaguje spolehlivěji než antivirový program (jedná-li se o nový virus, který dosud není ve virové databázi, antivirus jej nezachytí — *Kerio Personal Firewall* však vždy pozná, že došlo ke změně spustitelného souboru a upozorní uživatele).

Detekce útoků Systém detekce útoků (*IDS — Intrusion Detection System*) dokáže rozpoznat, blokovat a zaznamenat známé typy útoků. K tomuto účelu má *Kerio Personal Firewall* databázi známých útoků, která je pravidelně aktualizována (aktualizace je vždy začleněna do nové verze produktu).

Filtrování obsahu WWW stránek Modul pro filtrování obsahu umožňuje:

- blokování reklam (dle pravidel pro URL), skriptů a dalších prvků WWW stránek
- blokování pop-up oken
- blokování skriptů (*JavaScript*, *VB Script*)
- ochranu před ukládáním nežádoucích cookies a odesíláním privátních dat

Pro důvěryhodné servery či případy, kdy filtrování způsobí nefunkčnost určitých stránek, je možno definovat výjimky (specifická nastavení).

Mezi další významné funkce a vlastnosti *Kerio Personal Firewallu* patří:

Blokování veškeré komunikace *Kerio Personal Firewall* umožňuje jedním tlačítkem (resp. volbou z menu) zablokovat síťovou komunikaci počítače, na kterém je nainstalován (tzv. síťový zámek). Tuto funkci lze použít při zjištění podezřelé či nežádoucí síťové aktivity — po provedení příslušných opatření může být komunikace opět povolena.

Logování Každý z modulů firewallu vytváří vlastní záznam (log), který se ukládá jako soubor v textovém formátu. Záznamy lze prohlížet přímo v konfiguračním okně *Kerio Personal Firewallu*. Volitelně je možno záznamy také odesílat na *Syslog* server.

Přehled spojení a statistiky Přehled spojení dává uživateli informaci o navázaných spojeních a portech otevřených jednotlivými aplikacemi. U spojení se rovněž zobrazuje aktuální přenosová rychlost a celkový objem přenesených dat v každém směru. Seznam je automaticky obnovován v pravidelných intervalech.

1.2 Plná a volně šiřitelná verze

Statistiky informují uživatele o počtu objektů blokových WWW filtrem, počtu zachycených privátních informací a počtu detekovaných útoků za zvolené časové období.

Automatická aktualizace *Kerio Personal Firewall* pravidelně kontroluje, zda není k dispozici novější verze, a pokud ano, nabídne uživateli její stažení a instalaci. Kontrolu nové verze lze také kdykoliv provést ručně.

1.2 Plná a volně šiřitelná verze

Kerio Personal Firewall je k dispozici ve dvou verzích: plné (placené) a volně šiřitelné.

Instalační balík je pro obě verze společný. Po instalaci se produkt chová jako demoverze (tj. plná verze s časovým omezením na 30 dnů). Pokud nebude produkt během této doby zaregistrován, stává se z něj volně šiřitelná verze. Zakoupením licence a registrací produktu se z instalované demoverze nebo volně šiřitelné verze stává plná verze (podrobnosti viz kapitola 2.3).

Volně šiřitelná verze má oproti plné verzi tato omezení:

- Může být použita pouze pro osobní a/nebo nekomerční účely.
- Není funkční filtrování obsahu WWW stránek, včetně příslušných záznamů a statistik (viz kapitola 8).
- Nemůže být použita na internetové bráně (viz kapitola 4.2).
- Záznamy nelze odesílat na *Syslog* server (viz kapitola 10.3).
- Nemůže být provozována na operačních systémech serverového typu (tj. Windows NT Server, Windows 2000 Server a Windows Server 2003). Pokud byla demoverze instalována na některém z těchto systémů, pak se po vypršení třicetidenní lhůty zastaví služba *Personal Firewall Engine* a nebude již možné ji znovu spustit.

1.3 Systémové požadavky

Pro instalaci aplikace *Kerio Personal Firewall* je požadováno:

- CPU Intel Pentium nebo 100% kompatibilní
- 64 MB RAM

Kapitola 1 Úvod

- 8 MB místa na disku (pouze pro instalaci; doporučujeme dalších minimálně 10 MB pro soubory záznamů)
- operační systém Windows 98 / Me / NT 4.0 / 2000 / XP / Server 2003

1.4 Konfliktní software

Kerio Personal Firewall vykazuje konflikty s určitými druhy aplikací, které používají stejné nebo podobné technologie. Při kombinaci s níže uvedenými aplikacemi nezaručujeme správnou funkci *Kerio Personal Firewallu* ani operačního systému.

Neinstalujte *Kerio Personal Firewall* na tentýž operační systém společně s těmito aplikacemi:

Personální firewally Osobní firewally (např. *Internet Connection Firewall* — součást Windows XP, *Zone Alarm*, *Sygate Personal Firewall*, *Norton Personal Firewall* apod.) poskytují obdobnou funkčnost jako *Kerio Personal Firewall*. Rozhodnete-li se používat *Kerio Personal Firewall*, nekombinujte jej s dalšími firewallem.

Síťové firewally Síťový firewall (např. *Kerio WinRoute Firewall*, *Kerio WinRoute Pro*, *Kerio WinRoute Lite*, *Microsoft ISA Server*, *CheckPoint Firewall-1*, *WinProxy* firmy Ositis, *Sygate Office Network* a *Sygate Home Network* atd.) sám chrání také počítač, na kterém je nainstalován, a proto není třeba jej doplňovat personálním firewallem.

Poznámka: *Kerio Personal Firewall* může být kombinován se směrovačem, se směrovačem provádějícím překlad IP adres (NAT) nebo proxy serverem — např. *Internet Connection Sharing (Sdílené internetového připojení* — součást novějších verzí operačního systému Windows) za účelem vytvoření jednoduchého síťového firewallu. Podrobné informace naleznete v kapitole 4.2.

1.5 Instalace, upgrade a odinstalování

Instalace

Instalaci provedete jednoduše spuštěním instalačního programu (např. *kerio-pf-4.0.0-en-win.exe*). Během instalace můžete vybrat adresář, do kterého bude aplikace *Kerio Personal Firewall* nainstalována

(standardně C:\Program Files\Kerio\Personal Firewall 4).

Po instalaci je třeba systém restartovat, aby byl zaveden nízkourovňový ovladač *Kerio Personal Firewallu*.

1.6 Kontrola nových verzí

Poznámka: V operačních systémech Windows 98, Me, NT 4.0 a 2000 může být vyžadována aktualizace systémového instalátoru (*Windows Installer*), pokud již nebyl aktualizován dříve (např. při instalaci jiné aplikace). Velikost této aktualizace je cca 1.8 MB. Aktualizaci instalátoru je třeba stáhnout a nainstalovat, jinak nelze v instalaci aplikace *Kerio Personal Firewall* pokračovat!

Poznámka:

Při instalaci se v operačních systémech typu Windows NT zapíná vytváření výpisu paměti v případě havárie systému. Výpis paměti může uživatel odeslat do firmy *Kerio Technologies* — jeho analýza může pomoci k nalezení a odstranění chyby, která havárii operačního systému způsobila.

Po zaškrtnutí příslušné volby (viz kapitola 4.2) se v operačním systému nastaví generování výpisu paměti.

Upgrade

Instalace nové verze, resp. oprava stávající instalace se provádí stejným způsobem jako nová instalace (viz výše). Spuštěné komponenty aplikace není třeba ukončovat — instalační program je zastaví sám.

Poznámka: *Kerio Personal Firewall* má vestavěný mechanismus pro automatickou kontrolu a stahování nových verzí (podrobnosti viz kapitola 1.6).

Odinstalování

Kerio Personal Firewall lze odinstalovat pomocí nástroje *Přidat nebo odebrat programy* (*Add / Remove programs*) v *Ovládacích panelech* (*Control Panel*). Při odinstalování nebudou smazány soubory, které vznikly až za běhu aplikace (tj. konfigurační soubory, záznamy atd.). Ty je třeba smazat ručně, případně mohou zůstat uchovány pro další instalaci.

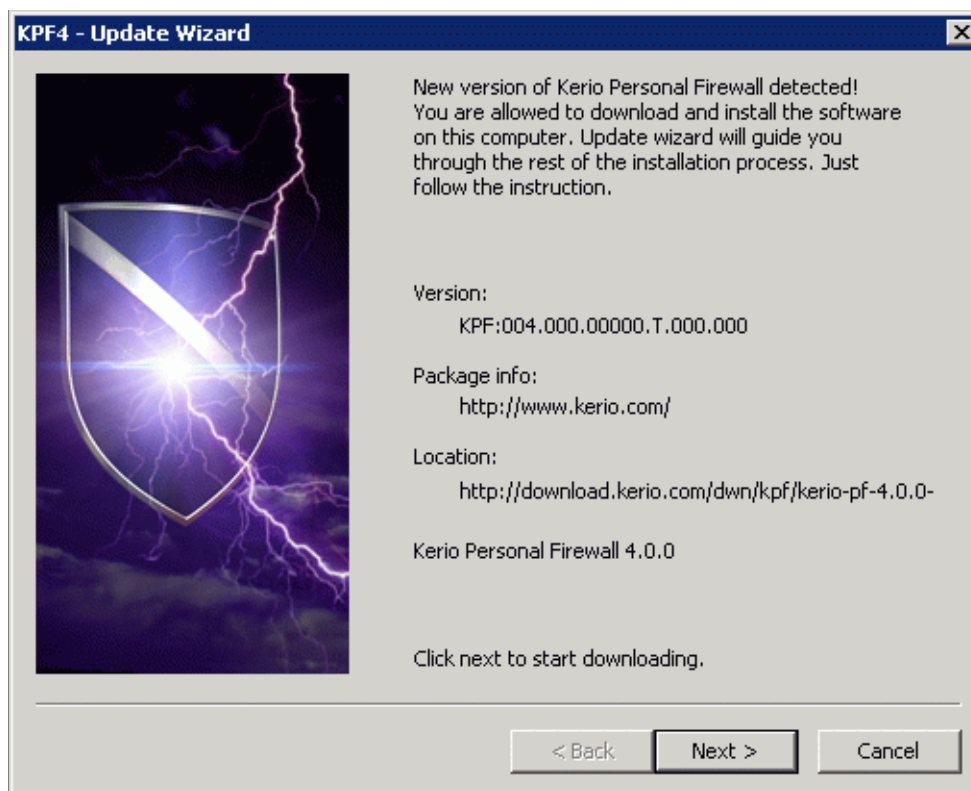
1.6 Kontrola nových verzí

Kerio Personal Firewall automaticky kontroluje, zda je k dispozici novější verze, a pokud ano, nabídne ji uživateli ke stažení. Kontrola nové verze se provádí při každém spuštění *Personal Firewall Engine* a pak pravidelně v intervalu 24 hodin. Nepodaří-li se z nějakého důvodu navázat spojení s aktualizacím serverem, bude se pokus o aktualizaci opakovat 1x za hodinu, dokud se spojení se serverem úspěšně nenaváže.

Kontrolu nové verze lze také kdykoliv spustit ručně tlačítkem *Check now* v sekci *Overview / Preferences* konfiguračního okna *Kerio Personal Firewallu* (podrobnosti viz kapitola 4.2).

Kapitola 1 Úvod

Je-li verze *Kerio Personal Firewallu* na vašem počítači aktuální, spojení se serverem se ukončí a naplánuje se příští kontrola nové verze. V opačném případě je zobrazen dialog s informacemi o nové verzi.



Stisknutím tlačítka *Next* se zahájí stahování nové verze. *Kerio Personal Firewall* vždy kontroluje signaturu staženého souboru — tím je zajištěno, že stažený soubor je skutečně originální (nejedná se o podvrh, není napaden virem, poškozen atd.).

Po stažení nové verze se spustí instalační program. Po instalaci je třeba počítač restartovat.

Tlačítkem *Cancel* lze stahování, resp. instalaci nové verze zrušit. V takovém případě nebude tato aktualizace znovu automaticky nabízena — lze ji však kdykoliv spustit ručně. Při nalezení další nové verze *Kerio Personal Firewall* opět nabídne aktualizaci automaticky.

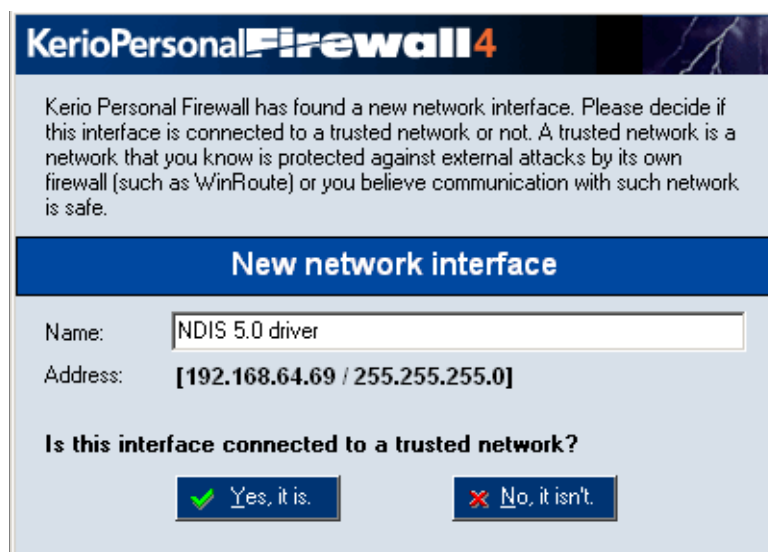
Podrobnosti o instalaci aplikace *Kerio Personal Firewall* naleznete v kapitole 1.5.

Poznámka: *Kerio Personal Firewall* má speciální interní pravidla, která vždy povolují přístup na server pro aktualizaci a registraci produktu. Uživatel tedy nemůže nevhodným nastavením firewallu automatickou aktualizaci zablokovat.

1.7 Počáteční konfigurace

Při prvním spuštění (tj. po instalaci) detekuje *Kerio Personal Firewall* aktivní síťová rozhraní počítače, na kterém je nainstalován. Pro každé rozhraní zobrazí dotaz, zda je toto rozhraní připojeno do důvěryhodné sítě či nikoliv.

Důvěryhodná síť je taková síť, o které uživatel předpokládá, že komunikace s počítači v ní je bezpečná. Typicky se jedná o lokální síť, která je proti průniku z Internetu chráněna síťovým firewallem. *Kerio Personal Firewall* umožňuje definovat různé akce pro důvěryhodnou síť a pro zbytek Internetu (podrobnosti viz kapitola 5.3).



V poli *Name* je uveden název příslušného síťového adaptéru, v položce *Address* jeho IP adresa a maska subsítě, do které je připojen.

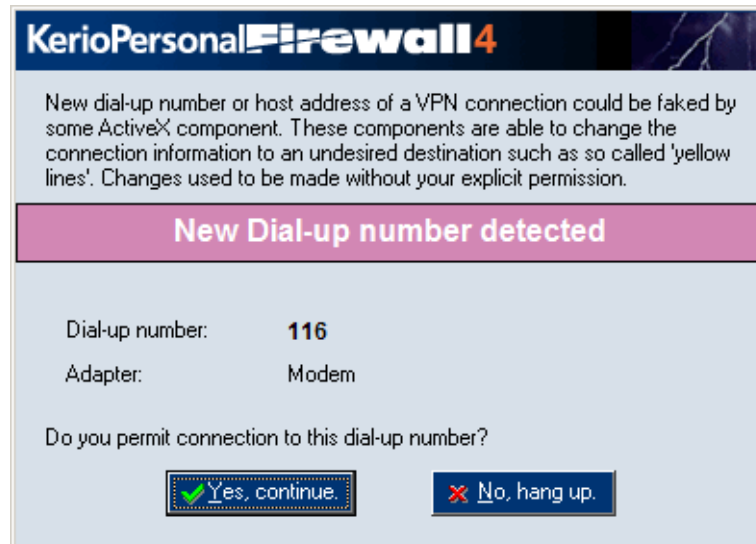
Stisknutím tlačítka *Yes, it is* se subsít', do níž je rozhraní připojeno, zařadí do skupiny důvěryhodných IP adres (*Trusted zone*). Tlačítko *No, it isn't* způsobí, že tato subsít' bude považována za součást Internetu.

Poznámky:

1. Nastavení skupiny důvěryhodných IP adres lze kdykoliv pozměnit (detailní informace naleznete v kapitole 5.3).
2. Je-li kdykoliv později přidáno či aktivováno další rozhraní nebo je rozhraní přepojeno do jiné subsítě, *Kerio Personal Firewall* jej rovněž automaticky detekuje a zobrazí výše popsany dialog.
3. V případě vytáčené linky se také kontroluje, zda od posledního vytočení nedošlo ke změně telefonního čísla. Jestliže *Kerio Personal Firewall* detekuje změnu čísla,

Kapitola 1 Úvod

dotáže se uživatele, zda tuto změnu akceptuje. Toto je ochrana proti nežádoucí změně parametrů telefonického připojení (např. ActiveX objektem na WWW stránce).



V poli *Dial-up number* je uvedeno nové telefonní číslo (tzn. telefonní číslo, které je nyní v příslušném telefonickém připojení nastaveno). Pole *Adapter* zobrazuje název telefonického připojení.

Po stisknutí tlačítka *Yes, continue* Kerio Personal Firewall změnu čísla akceptuje a povolí vytočení linky. Tlačítko *No, hang up* znamená zamítnutí změny — linka nebude vytočena.

Komponenty firewallu a základní ovládání

2.1 Komponenty aplikace Kerio Personal Firewall

Nízkoúrovňový ovladač Zavádí se do jádra operačního systému při jeho startu. Je umístěn mezi ovladači síťových rozhraní a TCP/IP subsystémem a zachytává a zpracovává veškerou přijatou či vysílanou IP komunikaci.

Nízkoúrovňový ovladač je uložen v systémovém adresáři Windows:

- v operačních systémech Windows NT a Windows 2000 typicky v adresáři C:\WINNT\system32\drivers (soubor fwdrv.sys)
- v operačním systému Windows XP typicky v adresáři C:\WINDOWS\system32\drivers (soubor fwdrv.sys)
- v operačních systémech Windows 98 a Windows Me typicky v adresáři C:\WINDOWS\system (soubor fwdrv.vxd)

Personal Firewall Engine Vlastní výkonné jádro *Kerio Personal Firewallu*. Běží jako služba nebo jako skrytá aplikace (Windows 98 a Me).

Služba *Personal Firewall Engine* je uložena v souboru *kpf4ss.exe* v instalačním adresáři aplikace *Kerio Personal Firewall*. Součástí *Personal Firewall Engine* je také tzv. rozhraní ovladače, které je uloženo v samostatném souboru *kfe.dll*.

Personal Firewall GUI Uživatelské rozhraní aplikace *Kerio Personal Firewall* (*GUI — Graphical User Interface*).

Komponentu *Personal Firewall GUI* spouští automaticky služba *Personal Firewall Engine* (při svém startu a dále v každém okamžiku, kdy detekuje, že uživatelské rozhraní neběží). Po spuštění se *Personal Firewall GUI* zobrazuje jako ikona tvaru štítu v pravé části nástrojové lišty (System Tray).

Pomocí ikony v System Tray lze otevřít konfigurační okno aplikace *Kerio Personal Firewall*, případně vyvolat některé další funkce (zablokování síťové komunikace, deaktivace firewallu atd.). Podrobnosti naleznete v kapitole 2.2.

Kapitola 2 Komponenty firewallu a základní ovládání



Komponenta *Personal Firewall GUI* je reprezentována souborem *kpf4gui.exe* v instalačním adresáři aplikace *Kerio Personal Firewall*.

Podpora rychlého přepínání uživatelů

Kerio Personal Firewall má vestavěnou podporu pro tzv. rychlé přepínání uživatelů ve Windows XP (*Fast User Switching*).

Personal Firewall GUI může běžet ve více instancích. *Personal Firewall Engine* vždy komunikuje s tou instancí, která náleží aktivnímu uživateli.

Po startu operačního systému a služby *Personal Firewall Engine* se spustí první instance, která běží pod systémovým účtem (resp. pod účtem, pod kterým se spouští služba *Personal Firewall Engine*). Při přihlášení uživatele se spustí nová instance *Personal Firewall GUI*, která běží s právy tohoto uživatele. Tato instance je aktivní až do odhlášení uživatele (v tom případě je ukončena), případně do přepnutí uživatelů (pak je pouze deaktivována).

2.2 Ikona na nástrojové liště

Ikona aplikace *Kerio Personal Firewall* v pravé části nástrojové lišty (System Tray) je zobrazena vždy, když běží komponenta *Personal Firewall GUI*. Tuto komponentu spouští automaticky služba *Personal Firewall Engine*.

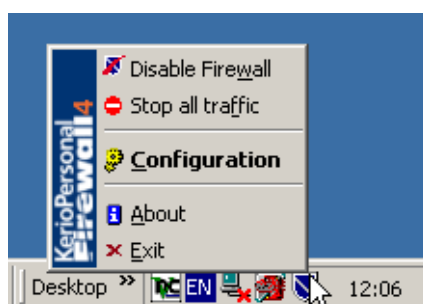
Ikona *Kerio Personal Firewallu* zobrazuje také síťovou aktivitu počítače, na kterém je firewall nainstalován. Síťová aktivita je zobrazována barevnými sloupci v dolní části ikony:



- zelený sloupec — odchozí (vysílaná) komunikace
- červený sloupec — příchozí (přijímaná) komunikace

Dvojitým kliknutím na ikonu levým tlačítkem myši se otevře konfigurační okno aplikace *Kerio Personal Firewall* (nastavení firewallu bude podrobně popsáno v kapitole 4). Po kliknutí na ikonu pravým tlačítkem myši se zobrazí menu s těmito funkcemi:

2.2 Ikona na nástrojové liště



Disable Firewall Deaktivace firewallu. Tato funkce vypíná všechny moduly *Kerio Personal Firewallu* — tj. filtrování síťové komunikace, sledování spouštěných aplikací, detekci útoků a filtrování obsahu WWW stránek.

Volba *Disable Firewall* je určena pro krátkodobé vyřazení firewallu, typicky pro účely testování či odstraňování problémů (např. nefunkčnost síťového připojení). Nedoporučujeme ponechávat volbu *Disable Firewall* trvale zapnutou — firewall je pak neúčinný a váš počítač není chráněn.

Je-li *Kerio Personal Firewall* deaktivován, ikona na nástrojové liště je červeně přeškrtnutá.



Výběrem funkce *Disable Firewall* se volba v menu se změní na *Enable Firewall* (povolit firewall) — výběrem této volby dojde k opětovné aktivaci firewallu.

Stop all traffic Zablokování veškeré síťové komunikace (tzv. síťový zámek).

Blokování síťové komunikace je signalizováno symbolem „jednosměrná ulice“ na ikoně *Kerio Personal Firewallu*.



Po aktivaci funkce *Stop all traffic* se volba v menu se změní na *Enable traffic* (povolit komunikaci) — výběrem této volby dojde k opětovnému povolení komunikace dle aktuálního nastavení firewallu.

TIP: Funkce *Stop all traffic* může být užitečná např. v případě, kdy omylem došlo k povolení síťové komunikace, která měla být zakázána. Volba *Stop all traffic* pozastaví aktuální spojení a zabrání navázání dalších spojení. Bylo-li vytvořeno komunikační

Kapitola 2 Komponenty firewallu a základní ovládání

pravidlo (tj. zaškrtnuta volba *Create a rule for this communication*), můžete jej smazat (viz kapitola 5.1, resp. 5.4) a poté komunikaci opět povolit.

Poznámka: Při startu služby *Personal Firewall Engine* se volby *Disable Firewall* a *Stop all traffic* vždy nastaví do výchozího stavu. Z bezpečnostních důvodů není žádoucí, aby byl firewall po startu neaktivní. Blokování veškeré komunikace by mohlo způsobit problémy např. s přihlašováním uživatelů.

Configuration Tato volba otevírá konfigurační okno aplikace *Kerio Personal Firewall*. Konfigurace firewallu je detailně popsána v kapitole 4.

About Okno „O aplikaci“. Obsahuje informace o verzích jednotlivých komponent *Kerio Personal Firewallu*, licenci, případně datu skončení funkčnosti časově omezené verze.

Exit Ukončení aplikace. Tato volba zastaví službu *Personal Firewall Engine* a ukončí všechny instance *Personal Firewall GUI* (tzn. uzavřou se všechna otevřená okna aplikace a skryje se ikona na nástrojové liště). Je-li v tomto okamžiku zobrazen alespoň jeden dialog (např. *Connection Alert*), čeká se na jeho potvrzení uživatelem.

Upozornění: Ukončením aplikace *Kerio Personal Firewall* přestává být váš počítač chráněn! *Kerio Personal Firewall* lze znovu aktivovat spuštěním služby v ovládacím panelu *Nástroje pro správu / Služby (Administrative Tools / Services)*.

2.3 Registrace produktu

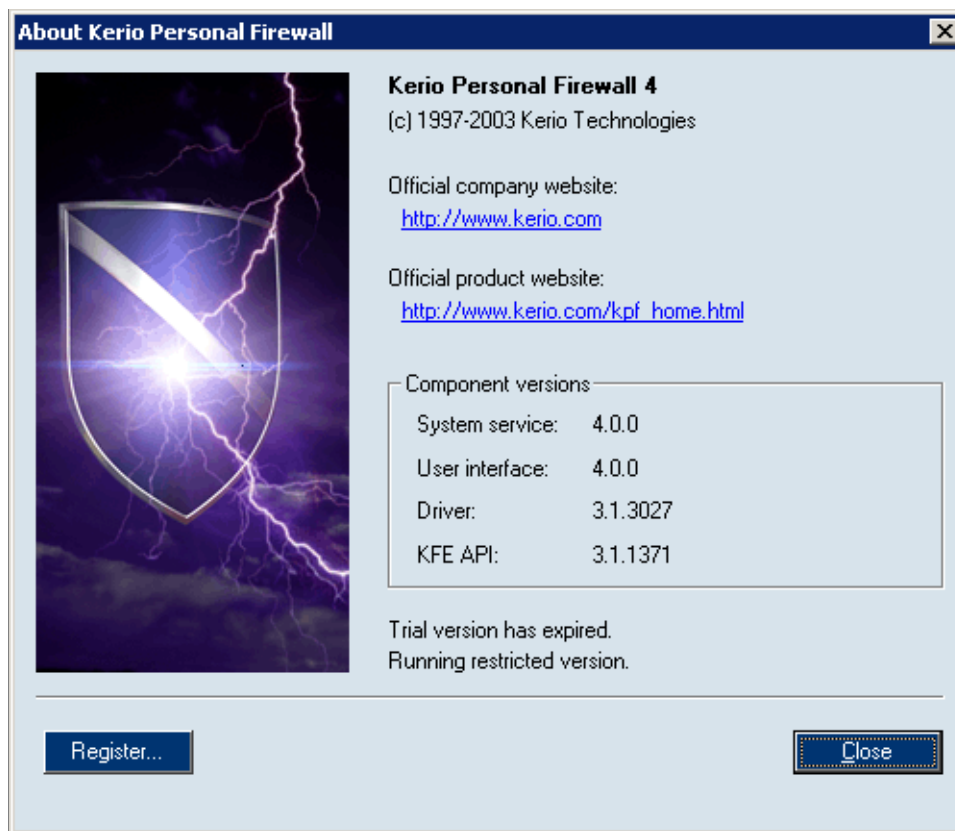
Zakoupenou licenci produktu *Kerio Personal Firewall* je třeba registrovat. Registrací se aktivují funkce, které nejsou ve volně šiřitelné verzi dostupné (viz kapitola 1.2), a uživatelé získávají nárok na plnou technickou podporu.

Poznámka: Produkt *Kerio Personal Firewall* je poskytován zdarma pro osobní a nekomerční použití. V takovém případě není nutné registraci provádět. Po uplynutí 30 dnů od instalace se však *Kerio Personal Firewall* začne chovat jako omezená verze — viz kapitola 1.2

Registraci *Kerio Personal Firewallu* lze provést na WWW stránkách firmy Kerio Technologies (<http://www.kerio.cz/>) nebo pomocí speciálního průvodce (*Registration Wizard*). Průvodce se spustí stisknutím tlačítka *Register...* v dialogu *About Kerio Personal Firewall* (tento dialog se otevírá volbou *About* z kontextového menu ikony na nástrojové liště — viz kapitola 2.2).

V prvním kroku průvodce je třeba vyplnit registrační číslo získané při zakoupení produktu (*Registration Key*).

2.3 Registrace produktu



Ve druhém kroku jsou požadovány informace o společnosti nebo osobě, na kterou je produkt registrován.

Položky *Company/Name* (název společnosti nebo jméno osoby) a *E-mail* (kontaktní e-mailová adresa) jsou povinné, tzn. musejí být vyplněny. Ostatní položky jsou volitelné.

Po stisknutí tlačítka *Next* naváže *Kerio Personal Firewall* spojení s registračním serverem, ověří správnost zadaných údajů a automaticky stáhne licenční klíč (digitální certifikát).

Ve třetím kroku průvodce se zobrazí informace o výsledku registrace.

Jedná-li se o časově omezenou licenci, zobrazí se datum skončení platnosti licence (*License expiration*) a skončení předplatného (*Subscription expiration*) — tj. nároku na bezplatné aktualizace produktu.

Stisknutím tlačítka *Finish* se průvodce ukončí.

Poznámka: Při dalším otevření dialogu *About Kerio Personal Firewall* se v levém dolním rohu okna namísto tlačítka *Register* zobrazí tlačítko *License info*, které otevírá okno s informacemi o licenci:

Kapitola 2 Komponenty firewallu a základní ovládání

KPF4 - Registration Wizard (step 2 of 3)

Please fill in the form below with the valid information. Red colored items are mandatory.

Company/Name: Kerio Technologies

Country: Czech Republic

Email: support@kerio.com

Contact person:

Street: Sedláčkova 16

City: Plzeň

Zip Code: 30111

Phone: +420 377 338 901

Website: http://www.kerio.com

Comment:

Click next to send the registration form to Kerio.

< Back Next > Cancel

KPF4 - License information

Serial number: 11111-22222-33333

Company: Kerio Technologies

Email: support@kerio.com

License expires: never


Subscription expires: 14/8/2004 13:00:00

Close

- *Serial number* — sériové číslo produktu
- *Company* — společnost, na kterou je produkt registrován
- *Email* — kontaktní e-mailová adresa
- *License expires* — datum skočení platnosti licence (*never* = platnost licence není časově omezena)
- *Subscription expires* — datum skončení platnosti předplatného, tj. nároku na bezplatné automatické aktualizace produktu

2.3 Registrace produktu

KPF4 - Registration Wizard (step 1 of 3) ✕



Please fill in your registration key you have purchased from our sales department. Then you will be able to register your copy of Kerio Personal Firewall.

Registration key: - -

Click next to proceed further with the registration form.

Chování firewallu a interakce s uživatelem

3.1 Chování firewallu

Při komunikaci v síti Internet se používají protokoly sady TCP/IP. Tyto protokoly jsou převážně používány i pro komunikaci v lokálních sítích. Základním (nosným) protokolem je IP (Internet Protocol), jehož pakety nesou veškeré další informace (zapouzdřují v sobě ostatní protokoly). *Kerio Personal Firewall* má úplnou kontrolu nad všemi IP pakety — tzn. je schopen je zachytit, zjistit z nich potřebné informace a poté je propustit nebo filtrovat. Samozřejmostí je také vytváření záznamů o prováděných akcích, detekovaných útocích apod.

Základním principem činnosti *Kerio Personal Firewallu* je tzv. stavová inspekce. Probíhala-li komunikace protokolem TCP, pak je o každém povoleném spojení vytvořen záznam, a firewall propustí pouze pakety patřící do tohoto spojení.

Kerio Personal Firewall pracuje v tzv. samoučícím režimu. Při zachycení dosud neznámé síťové komunikace se zobrazí dialogové okno, ve kterém může uživatel příslušnou komunikaci povolit či zakázat, a to jednorázově nebo trvale. Pro trvale povolenou či zakázanou komunikaci se automaticky vytvoří odpovídající pravidlo a při příštím zachycení této komunikace se již *Kerio Personal Firewall* uživatele nedotazuje. Detaily naleznete v kapitolách 3.2 a 5.4.

Filtrovacími pravidly může uživatel (resp. administrátor) specifikovat další podmínky pro filtrování komunikace. Vždy jsou ale propuštěny jen takové pakety, které vyhovují definovaným kritériím.

Obdobným způsobem *Kerio Personal Firewall* postupuje také při kontrole spouštěných aplikací (podrobnosti viz kapitola 6.1).

3.2 Dialog Connection Alert (zachycení neznámé komunikace)

Dialog *Connection Alert* (dotaz na povolení či zákaz komunikace) informuje uživatele o tom, že *Kerio Personal Firewall* zachytil dosud neznámou komunikaci a očekává jeho rozhodnutí, zda tuto komunikaci povolit či zakázat, případně vytvořit odpovídající komunikační pravidlo.

Poznámka: Chování *Kerio Personal Firewallu* při zachycení síťové komunikace určují volby a pravidla v sekci *Network Security* (viz kapitoly 5.1 a 5.2). Dialog *Connection Alert*

Kapitola 3 Chování firewallu a interakce s uživatelem

se zobrazuje v případech, kdy neexistuje odpovídající pravidlo nebo pravidlo explicitně vyžaduje dotázat se uživatele.

Tento dialog je zobrazen vždy nad okny ostatních aplikací („Always on Top“). Je-li zachyceno více událostí (tj. více pokusů o navázání spojení nebo spuštění aplikací — viz kapitola 3.3) současně, pak se tyto události řadí do fronty — teprve po potvrzení jednoho dialogu se zobrazí další; nikdy se nezobrazuje více dialogů *Connection Alert* současně.



Dialog *Alert* obsahuje následující informace a volby:

Směr komunikace a zóna Barevný pruh v horní části dialogu informuje uživatele o směru komunikace (příchozí nebo odchozí) a zóně, do které patří vzdálený počítač (důvěryhodné IP adresy nebo Internet).



3.2 Dialog Connection Alert (zachycení neznámé komunikace)

Barva pruhu a text před závorkou určuje směr navazovaného spojení:

- *Outgoing connection alert* — odchozí spojení (tzn. navazované z lokálního počítače na vzdálený).

Odchozí spojení je signalizováno zelenou barvou.

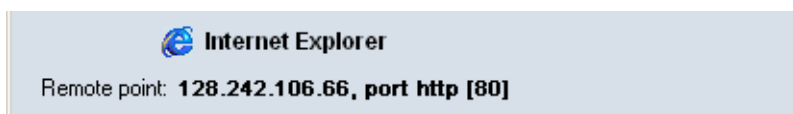
- *Incoming connection alert* — příchozí spojení (tzn. navazované ze vzdáleného počítače na lokální).

Příchozí spojení je signalizováno červenou barvou.

V závorce je uvedena zóna, do které patří IP adresa vzdáleného počítače:

- *Trusted area* — skupina důvěryhodných IP adres (podrobnosti viz kapitola 5.3)
- *Internet* — „zbytek světa“ (tj. libovolná IP adresa, která nepatří do skupiny *Trusted area*)

Lokální aplikace a vzdálený konec spojení Pod barevným pruhem s informací o směru komunikace jsou uvedeny stručné informace o navazovaném spojení:



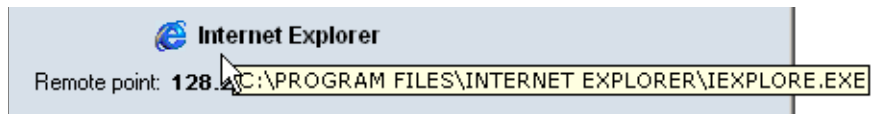
- ikona a popis aplikace na lokálním počítači. Není-li popis k dispozici, zobrazí se jméno spustitelného souboru aplikace. Nemá-li aplikace svoji ikonu, použije se standardní systémová ikona pro spustitelné soubory.
- DNS jméno vzdáleného počítače a jeho IP adresa (v hranatých závorkách).

Poznámka: DNS jména počítačů se zjišťují dotazováním DNS. V závislosti na rychlosti odezvy může být po nějakou dobu zobrazena pouze IP adresa daného počítače. Pokud neexistuje odpovídající DNS záznam, zůstane trvale zobrazena pouze IP adresa. Převod IP adres na DNS jména lze globálně vypnout/zapnout např. v kontextovém menu okna *Overview / Connections* (viz kapitola 9.1)

- vzdálený port (jedná-li se o standardní službu, zobrazí se její jméno a číslo portu v hranatých závorkách; jinak číslo portu bez závorek)

Při umístění kurzoru myši na popis aplikace se jako nápovědný text (tooltip) zobrazí úplná cesta k spustitelnému souboru aplikace.

Kapitola 3 Chování firewallu a interakce s uživatelem



Volba akce Nejdůležitější částí dialogu je volba akce, tedy povolení či zakázání příslušné komunikace.



- Tlačítko *Permit* povolí danou komunikaci.
- Tlačítko *Deny* zakáže danou komunikaci.
- Volba *Create a rule for this communication and don't ask me again* způsobí vytvoření komunikačního pravidla na základě zachycené komunikace. Akce v pravidle bude nastavena podle toho, které tlačítko bylo stisknuto (*Permit* nebo *Deny*). Při příštím zachycení stejné komunikace se již *Kerio Personal Firewall* nebude dotazovat uživatele, ale provede akci dle vytvořeného komunikačního pravidla.

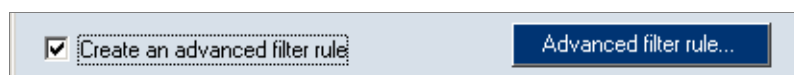
Poznámka: Vytvořené komunikační pravidlo lze kdykoliv později upravit nebo odstranit v okně *Kerio Personal Firewall Administration* v sekci *Network Security*, záložka *Applications*. Podrobnosti naleznete v kapitole 5.1.

- Tlačítko *Details* zobrazí pole s podrobnými informacemi o navazovaném spojení a lokální aplikaci. Opětovným stisknutím tohoto tlačítka se podrobné informace skryjí.

Následující části dialogu se zobrazí po stisknutí tlačítka *Details*.

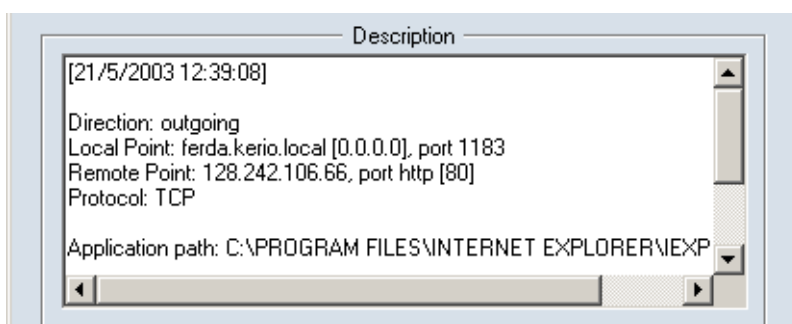
Detailní informace o spojení a lokální aplikaci V poli *Description* jsou uvedeny podrobné informace o spojení (směr, protokol, lokální a vzdálená IP adresa, lokální a vzdálený port) a lokální aplikaci, která se komunikace účastní (jméno spustitelného souboru aplikace včetně plné cesty, popis aplikace, datum vytvoření, poslední změny a poslední čtení spustitelného souboru).

Vytvoření rozšířeného pravidla



Zaškrtnutím volby *Create an advanced filter rule* bude namísto standardního pravidla pro aplikaci (viz kapitola 5.1) vytvořeno pravidlo rozšířeného paketového filtru,

3.3 Dialog Starting/Replacing/Launching other application



umožňující detailně nastavit parametry komunikace (IP adresy, porty atd.), lokální aplikaci, časovou platnost atd.

Tlačítko *Advanced filter rule...* otevírá dialog pro definici pravidla paketového filtru, ve kterém lze pravidlo upravit (upřesnit) dle požadavků uživatele. Rozšířené pravidlo lze kdykoliv změnit nebo odstranit v okně *Kerio Personal Firewall Administration* (sekce *Network Security*, záložka *Applications*, tlačítko *Packet filter*).

Podrobnosti o rozšířených komunikačních pravidlech naleznete v kapitole 5.4.

Poznámka: Po dobu, kdy je zobrazen dialog *Connection Alert*, je příslušná komunikace „pozastavena“ (již přijatá či vyslaná data uchovává *Kerio Personal Firewall* ve své vyrovnávací paměti). Ne-li reakce uživatele dostatečně rychlá, může vysílající aplikace po určité době (zpravidla několik desítek sekund) tento stav vyhodnotit jako síťovou chybu (cílový počítač nedostupný).

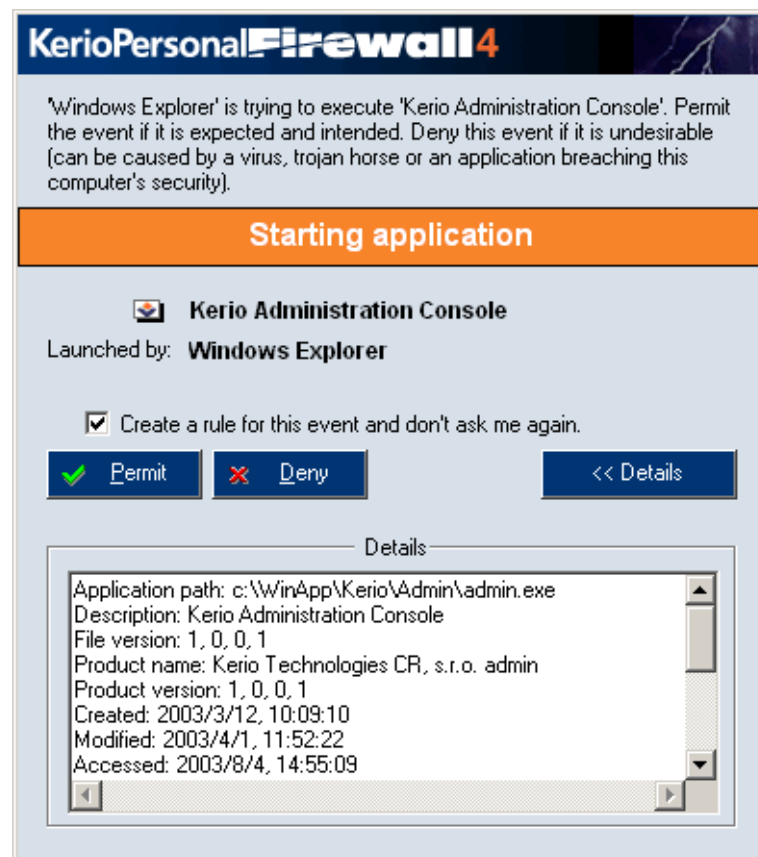
3.3 Dialog Starting/Replacing/Launching other application

Dialog *Starting/Replacing/Launching other application* (upozornění na spuštění nebo záměnu aplikace, resp. spuštění aplikace jinou aplikací) informuje uživatele o tom, že *Kerio Personal Firewall* detekoval pokus o spuštění aplikace a očekává jeho rozhodnutí, zda tuto akci povolit či zakázat, případně vytvořit odpovídající pravidlo. Aplikace bude spuštěna až v okamžiku, kdy to uživatel povolí.

Poznámka: Chování *Kerio Personal Firewallu* při spouštění aplikací určují volby a pravidla v sekci *System Security* (viz kapitola 6). Dialog *Starting/Replacing/Launching other application* se zobrazuje v případech, kdy neexistuje odpovídající pravidlo nebo pravidlo explicitně vyžaduje dotázat se uživatele.

Tento dialog je zobrazen vždy nad okny ostatních aplikací („Always on Top“). Je-li zachyceno více událostí (tj. více pokusů o spuštění aplikací nebo o síťovou komunikaci — viz kapitola 3.2) současně, pak se tyto události řadí do fronty — teprve po potvrzení jednoho dialogu se zobrazí další. Nikdy se tedy nezobrazuje více dialogů *Starting/Replacing/Launching other application* a/nebo *Connection Alert* současně.

Kapitola 3 Chování firewallu a interakce s uživatelem



Dialog obsahuje tyto informace:

Popis události V záhlaví dialogového okna je uveden slovní popis zachycené události a obecné doporučení, jakou akci by měl uživatel zvolit.

'Windows Explorer' is trying to execute 'Kerio Administration Console'. Permit the event if it is expected and intended. Deny this event if it is undesirable (can be caused by a virus, trojan horse or an application breaching this computer's security).

Název události Barevný pruh obsahuje informaci o tom, jaká událost byla zachycena:

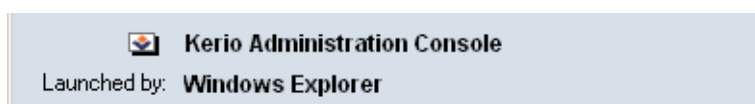
Starting application

- *Starting application* — spuštění aplikace
- *Replacing application* — změna ve spustitelném souboru aplikace
- *Application is launching other application* — běžící aplikace spouští jinou aplikaci

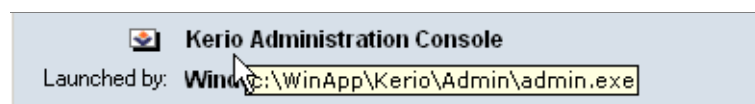
3.3 Dialog Starting/Replacing/Launching other application

Ikona a popis aplikace Pod informací o typu události je zobrazen popis a ikona spouštěné aplikace. Není-li popis k dispozici, zobrazí se jméno spustitelného souboru aplikace. Nemá-li aplikace svoji ikonu, použije se standardní systémová ikona pro spustitelné soubory.

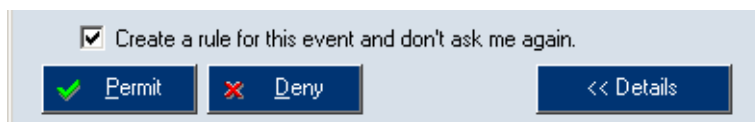
Pokud byla aplikace spuštěna jinou aplikací, zobrazí se ve druhém řádku (*Launched by*) popis této aplikace.



Při umístění kurzoru myši na popis aplikace (v prvním řádku) nebo na popis aplikace, která ji spouští (ve druhém řádku) se jako nápovědný text (tooltip) zobrazí úplná cesta k spustitelnému souboru aplikace.

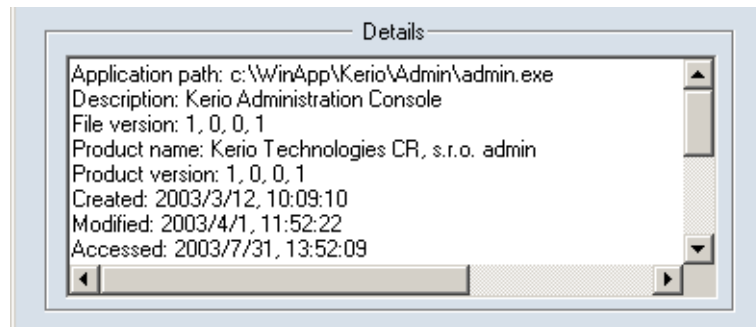


Volba akce Nejdůležitější částí dialogu je volba akce — tedy povolení či zakázání spuštění příslušné aplikace.



- Tlačítko *Permit* povolí spuštění aplikace.
- Tlačítko *Deny* zakáže spuštění aplikace.
- Volba *Create a rule for this event and don't ask me again* způsobí vytvoření pravidla pro tuto událost (v sekci *System Security / Applications*). Při příštím zachycení události stejného typu se již firewall uživatele nedotazuje a provede akci definovanou uživatelem.
- Tlačítko *Details* zapíná/vypíná zobrazení podrobnosti o spouštěné aplikaci (případně také o aplikaci, která ji spouští)

Podrobnosti o aplikacích Sekce *Details* obsahuje podrobné informace o spouštěné aplikaci, případně o aplikaci, která se ji pokouší spustit (úplná cesta k spustitelnému souboru, popis aplikace, číslo verze, datum vytvoření, poslední změny a posledního přístupu k souboru atd.).

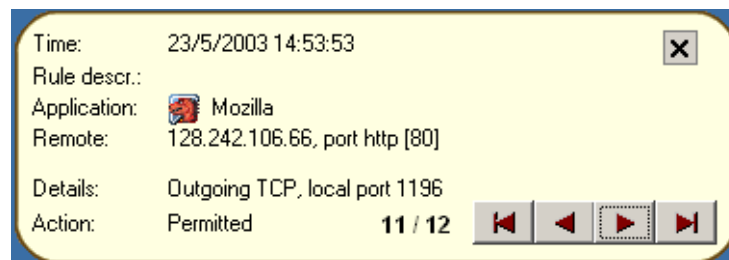


3.4 Okno Alert (upozornění na událost)

V pravidlech *Kerio Personal Firewallu* může být nastaveno zobrazení upozornění (*Alert*) při zachycení komunikace vyhovující tomuto pravidlu, resp. při spuštění odpovídající aplikace. Jestliže *Kerio Personal Firewall* zaznamená takovou událost, zobrazí v pravém dolním rohu obrazovky okno s detailními informacemi. Nastanou-li další události tohoto typu dříve, než uživatel informační okno zavře, řadí se informace do fronty, kterou lze procházet oběma směry (použitím tlačítek se šipkami v pravém dolním rohu okna).

Upozornění: Uzavřením okna *Alert* (kliknutím na křížek v pravém horním rohu nebo kombinací kláves *Alt+F4*) dojde k vymazání všech zpráv z fronty, bez ohledu na to, zda byly zobrazeny či nikoliv!

Příklad upozornění na síťovou komunikaci



Zpráva v okně *Alert* obsahuje tyto položky:

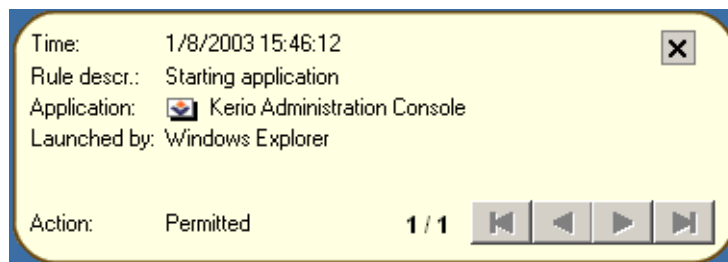
- *Time* — datum a čas, kdy událost nastala
- *Rule descr.* — popis (název) komunikačního pravidla, které bylo uplatněno
- *Application* — ikona a název lokální aplikace, která se komunikace účastní (nemá-li aplikace ikonu, použije se standardní systémová ikona; není-li k dispozici název aplikace, zobrazí se jméno spustitelného souboru bez přípony)

3.4 Okno Alert (upozornění na událost)

- *Remote* — IP adresa a port vzdáleného počítače (pokud lze z DNS zjistit jeho jméno, zobrazuje se namísto IP adresy; jedná-li se o standardní službu, zobrazí se před číslem portu její název)
- *Details* — podrobnosti o spojení: směr (*Outgoing* — odchozí, *Incoming* — příchozí), protokol a lokální port
- *Action* — akce, která byla provedena (*Permitted* — komunikace povolena, *Denied* — komunikace zakázána)
- pořadí zprávy ve frontě a celkový počet zpráv ve frontě (celkový počet zpráv může narůstat, jestliže v době zobrazení okna *Alert* generuje *Kerio Personal Firewall* další zprávy)

Podrobné informace o pravidlech pro síťovou komunikaci aplikací naleznete v kapitole 5.1.

Příklad upozornění na spouštění aplikace



Okno *Alert* obsahuje tyto položky:

- *Time* — datum a čas, kdy událost nastala
- *Rule descr.* — popis události, která byla zachycena:
 - *Starting application* — spouštění aplikace
 - *Replacing application* — změna spustitelného souboru aplikace
 - *Application is launching other application* — běžící aplikace spouští jinou aplikaci
- *Application* — ikona a název spouštěné aplikace (nemá-li aplikace ikonu, použije se standardní systémová ikona; není-li k dispozici název aplikace, zobrazí se jméno spustitelného souboru bez přípony)

Kapitola 3 Chování firewallu a interakce s uživatelem

- *Launched by* — název (popis) aplikace, která danou aplikaci spouští
- *Action* — akce, která byla provedena na základě odpovídajícího pravidla (*Permitted* — spuštění aplikace povoleno, *Denied* — spuštění aplikace zamítnuto).

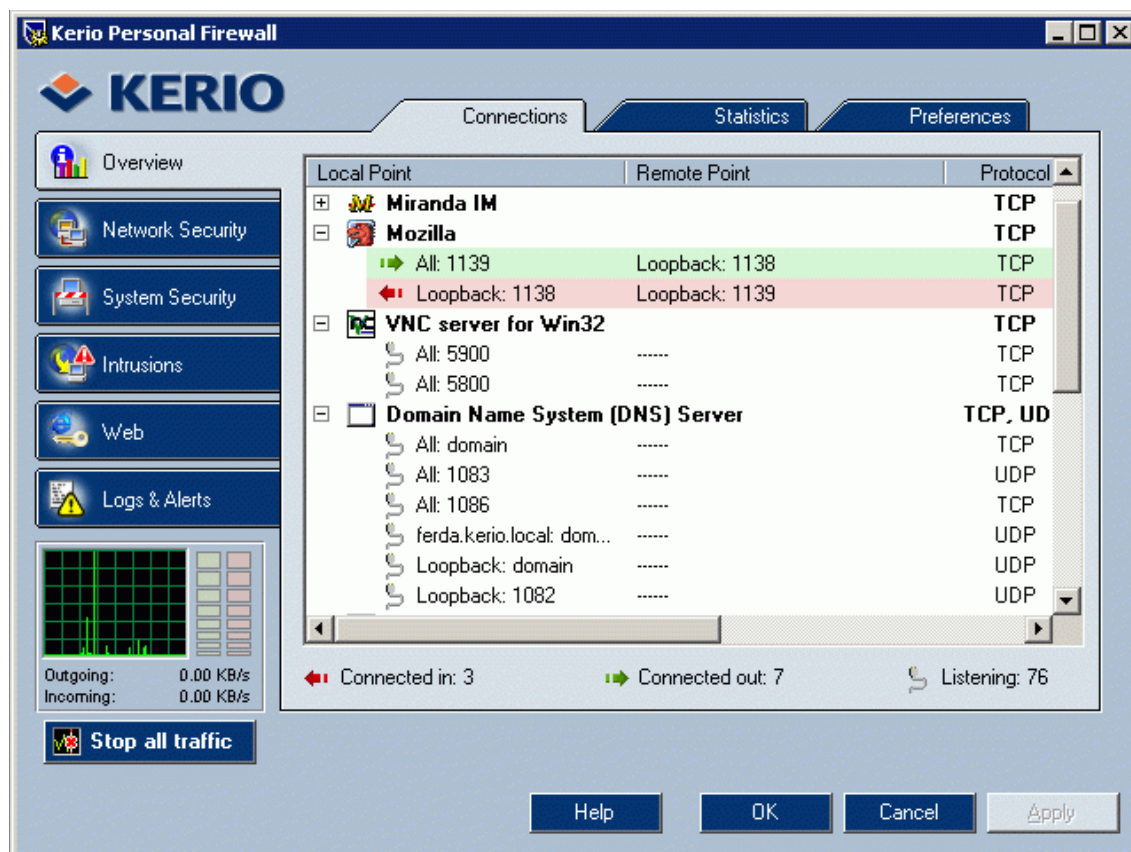
Podrobné informace o pravidlech pro spuštění aplikací naleznete v kapitole 6.1.

Konfigurace firewallu

4.1 Konfigurační okno

K nastavení *Kerio Personal Firewallu* a sledování stavových informací a záznamů slouží tzv. konfigurační okno. Toto okno lze otevřít následujícími způsoby:

- dvojitým kliknutím *levým* tlačítkem na ikonu *Kerio Personal Firewallu* na nástrojové liště
- kliknutím pravým tlačítkem na tuto ikonu a volbou *Configuration* z kontextového menu



Kapitola 4 Konfigurace firewallu

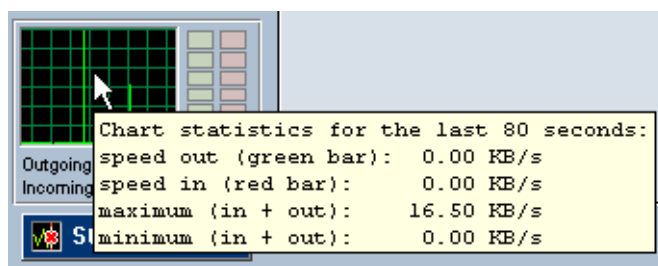
Záložky v levé části okna slouží k přepínání jednotlivých sekcí:

- *Overview* — přehled aktivních spojení a otevřených portů (viz kapitola 9.1), statistiky (viz kapitola 9.2) a uživatelské preference (viz kapitola 4.2).
- *Network Security* — pravidla pro síťovou komunikaci aplikací, paketový filtr, definice důvěryhodné zóny (viz kapitola 5)
- *System Security* — pravidla pro spuštění aplikací (viz kapitola 6)
- *Intrusions* — nastavení detekce známých typů útoků (viz kapitola 7)
- *Web* — pravidla pro WWW stránky — blokování pop-up oken, URL filtr, blokování objektů, kontrola nad odesílanými daty (viz kapitola 8)
- *Log & Alerts* — prohlížení a nastavení záznamů (viz kapitola 10)

Graf v levé dolní části okna zobrazuje časový průběh zatížení síťového rozhraní. Zelený sloupec vedle grafu zobrazuje aktuální (okamžitou) rychlost odchozí komunikace, červený sloupec rychlost příchozí komunikace.

Kliknutím levým tlačítkem myši na graf se přepíná zobrazení — čárový graf nebo plošný graf.

Při umístění kurzoru myši nad graf se zobrazí nápovědný text (tooltip) se statistikou síťové komunikace:



- *speed out (green bar)* — aktuální rychlost odchozí komunikace (zelený sloupec)
- *speed in (red bar)* — aktuální rychlost příchozí komunikace (červený sloupec)
- *maximum (in+out)* — nejvyšší zaznamenaná rychlost (součet odchozí a příchozí komunikace za posledních 80 sekund)
- *minimum (in+out)* — nejnižší zaznamenaná rychlost (součet odchozí a příchozí komunikace za posledních 80 sekund)

Tlačítko *Stop all traffic* (zastavit veškerou komunikaci) pod grafem slouží k zablokování veškeré síťové komunikace (všechna otevřená spojení budou pozastavena). Tato funkce může být užitečná např. v případě, kdy omylem povolíme komunikaci, která měla být zakázána. Po stisknutí změní toto tlačítko popis na *Enable traffic* (povolit komunikaci).

Je-li komunikace zastavena, je tento stav signalizován ikonou a textem pod tlačítkem *Enable traffic*.

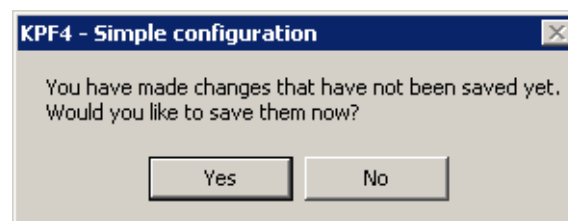


Poznámka: Volba *Stop all traffic* / *Enable traffic* je dostupná také z kontextového menu ikony *Kerio Personal Firewallu* na nástrojové liště (viz kapitola 2.2).

Tlačítka na spodním okraji okna mají standardní funkce:

- *OK* — uložení provedených změn a zavření konfiguračního okna
- *Cancel* — zavření okna bez uložení změn
- *Apply* — uložení (akceptování) provedených změn, okno zůstává otevřené
- *Help* — otevření nápovědy pro aktuální sekci/záložku

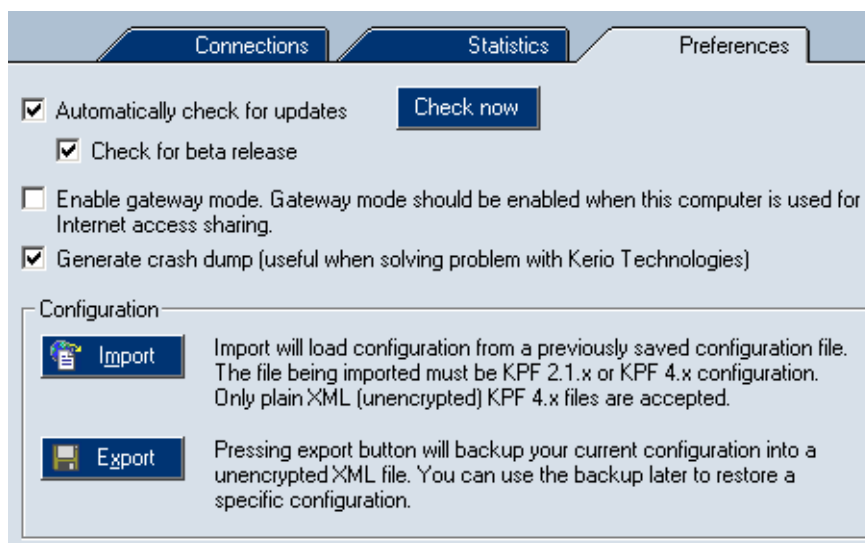
Poznámka: Změny konfigurace lze provádět současně pouze v jedné záložce jedné sekce. Při přechodu do jiné záložky, resp. jiné sekce se kontroluje, zda v aktuálním zobrazení nebyly provedeny dosud neuložené změny. Pokud ano, *Kerio Personal Firewall* se dotáže, zda má tyto změny akceptovat nebo stornovat.



4.2 Preference

Sekce *Overview* / *Preferences* slouží k nastavení uživatelských preferencí a upřesňujících parametrů firewallu.

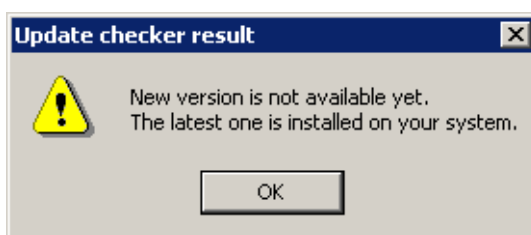
Kapitola 4 Konfigurace firewallu



Automatically check for updates Zapnutí/vypnutí automatické kontroly nových verzí programu. Pro zajištění maximální bezpečnosti doporučujeme ponechat tuto volbu zapnutou (nové verze obsahují aktualizace databáze známých útoků, opravy případných chyb atd.).

Podrobnosti o automatické kontrole a instalaci nové verze naleznete v kapitole 1.6.

Check now Toto tlačítko spouští okamžitou kontrolu existence nové verze *Kerio Personal Firewallu*. Je-li na aktualizacím serveru nalezena novější verze, pak je uživateli nabídnuto její stažení a instalace (podrobnosti viz kapitola 1.6). V opačném případě se zobrazí informace o tom, že novější verze není k dispozici (instalovaná verze je aktuální).



Check for beta release Zapnutím této volby budou při kontrole nových verzí uživateli nabízeny také zveřejněné betaverze. Betaverze jsou nové verze ve stádiu vývoje — není zaručena jejich plná funkčnost a mohou obsahovat chyby.

Volbu *Check for beta release* použijte v případě, jestliže se chcete účastnit testování betaverzí (podrobnosti viz <http://www.kerio.cz/>, *Beta Sekce*). Nemáte-li zájem o testování a chcete-li mít na svém počítači vždy plně funkční (finální) verzi, pak tuto volbu nezapínejte.

Enable gateway mode Tato volba přepíná firewall do speciálního režimu ochrany internetové brány (tj. směrovače nebo směrovače s překladem IP adres).

Po zapnutí volby *Enable gateway mode* bude *Kerio Personal Firewall* propouštět pakety s cílovými porty, na kterých neběží žádná lokální aplikace, případně pakety s cílovými IP adresami, které nejsou lokální.

Není-li *Kerio Personal Firewall* skutečně nasazen na internetové bráně, pak by tato volba měla být vypnuta, jinak degraduje ochranu lokálního počítače!

Poznámky:

1. Volbu *Enable Gateway Mode* lze také využít pro povolení síťové komunikace operačního systému, který je provozován v rámci programu *VMWare* (<http://www.vmware.com/>), jestliže *Kerio Personal Firewall* chrání hostitelský systém. Bude-li tato volba vypnuta, bude *Kerio Personal Firewall* blokovat pakety určené operačnímu systému uvnitř *VMWare*.
2. Je-li *Kerio Personal Firewall* použit k ochraně proxy serveru, není třeba tuto volbu zapínat (proxy server se chová jako klient na lokálním počítači).

Generate crash dump Zapnutí/vypnutí vytváření ladicích informací pro případ havárie *Kerio Personal Firewall*. Dojde-li po zapnutí této volby k pádu *Personal Firewall Engine* nebo *Personal Firewall GUI*, vytvoří se soubor s výpisem paměti a následně automaticky spustí utilita *Assist*, která nabídne odeslání informací o pádu (komprimovaného výpisu paměti a vybraných záznamů) k analýze do firmy *Kerio Technologies*.

V případě, že došlo k havárii operačního systému, může *Kerio Personal Firewall* po opětovném startu odeslat k analýze výpis paměti jádra (resp. úplný výpis paměti v případě Windows NT 4.0). 1 minutu po startu služby *Personal Firewall Engine* se provede kontrola, zda se na disku nenalézá nový výpis paměti. Pokud ano, spustí se utilita *Assist*. Ta se nejprve uživatele dotáže, zda se domnívá, že tento výpis má souvislost s pádem aplikace firmy *Kerio Technologies*, a v případě kladné odpovědi nabídne jeho odeslání k analýze. Výpis paměti je odeslán v komprimované podobě.

Poznámka: Odeslané informace budou použity výhradně pro účely ladění aplikace *Kerio Personal Firewall*. Nebudou použity k žádnému jinému účelu ani poskytnuty třetí straně.

Configuration Tato sekce obsahuje tlačítka pro zálohování konfigurace *Kerio Personal Firewall* a její obnovení, případně načtení konfigurace aplikace *Kerio Personal Firewall 2.1.x*.

Kapitola 4 Konfigurace firewallu

Po stisku tlačítka *Import* se zobrazí systémový dialog pro otevření souboru. *Kerio Personal Firewall* dokáže otevřít a načíst konfigurační soubor ve formátu:

- *Kerio Personal Firewall 4.x* v nešifrované podobě (formát XML, přípona `.cfg`)
- *Kerio Personal Firewall 2.1.x* (přípona `.conf`) — import konfigurace ze starší verze

Tlačítko *Export* otevírá systémový dialog pro uložení souboru. Takto je možné uložit konfigurační soubor (v nešifrované podobě) pro pozdější použití či pro přenos na jiný počítač.

Poznámka: Konfigurační soubor v šifrované podobě nelze importovat.

4.3 Pravidla firewallu

Při zachycení komunikace aplikují jednotlivé moduly firewallu definovaná pravidla v určeném pořadí. Jestliže komunikace vyhovuje určitému pravidlu, provede se odpovídající akce a vyhodnocování se ukončí.

Pravidla jednotlivých modulů *Kerio Personal Firewallu* se aplikují v tomto pořadí:

1. Systém detekce útoků (IDS — viz kapitola 7)
2. Interní pravidla pro komponenty *Kerio Personal Firewallu* — např. povolení přístupu na WWW server pro kontrolu a stahování nových verzí programu
3. Pravidla rozšířeného paketového filtru (viz kapitola 5.4)
4. Předdefinovaná pravidla pro síťovou komunikaci (viz kapitola 5.2)
5. Pravidla pro aplikace (viz kapitola 5.1)

Poznámka: Jednotlivé moduly firewallu lze vypnout — pak se příslušná pravidla na zachycenou komunikaci neaplikují. Interní pravidla firewallu vypnout nelze.

Pravidla pro síťovou komunikaci

Klíčovým bodem konfigurace *Kerio Personal Firewallu* jsou pravidla pro síťovou komunikaci. K dispozici jsou tři typy pravidel:

- *Pravidla pro aplikace* — jednoduchá pravidla definující chování firewallu při síťové komunikaci s počítači v důvěryhodné zóně a v Internetu. Tato pravidla jsou vytvářena automaticky na základě reakce uživatele při zachycení dosud neznámé síťové komunikace. Podrobnosti viz kapitola 5.1.
- *Rozšířený paketový filtr* — detailní pravidla pro síťovou komunikaci (možnost nastavení IP adres, protokolu, portů, aplikace atd.). Pravidla paketového filtru mohou být definována buď ručně (v konfiguračním okně *Kerio Personal Firewallu*) nebo automaticky na základě reakce uživatele (viz kapitola 3.2)

Nastavení rozšířeného paketového filtru je popsáno v kapitole 5.4.

- *Předdefinovaná pravidla pro síťovou komunikaci* — *Kerio Personal Firewall* obsahuje sadu předdefinovaných pravidel, která jsou nezávislá na aplikacích. U předdefinovaných pravidel může uživatel nastavovat pouze akci (tj. povolit nebo zakázat příslušnou komunikaci). Předdefinovaná pravidla lze jednoduše zapnout nebo vypnout (jedna volba pro všechna pravidla). Podrobnosti viz kapitola 5.2.

Modul firewallu pro kontrolu síťové komunikace lze zapnout/vypnout volbou *Enable Network Security module* v sekci *Network Security*, záložka *Applications*. Je-li tato volba vypnuta, pak jsou všechny uvedené typy pravidel neaktivní.

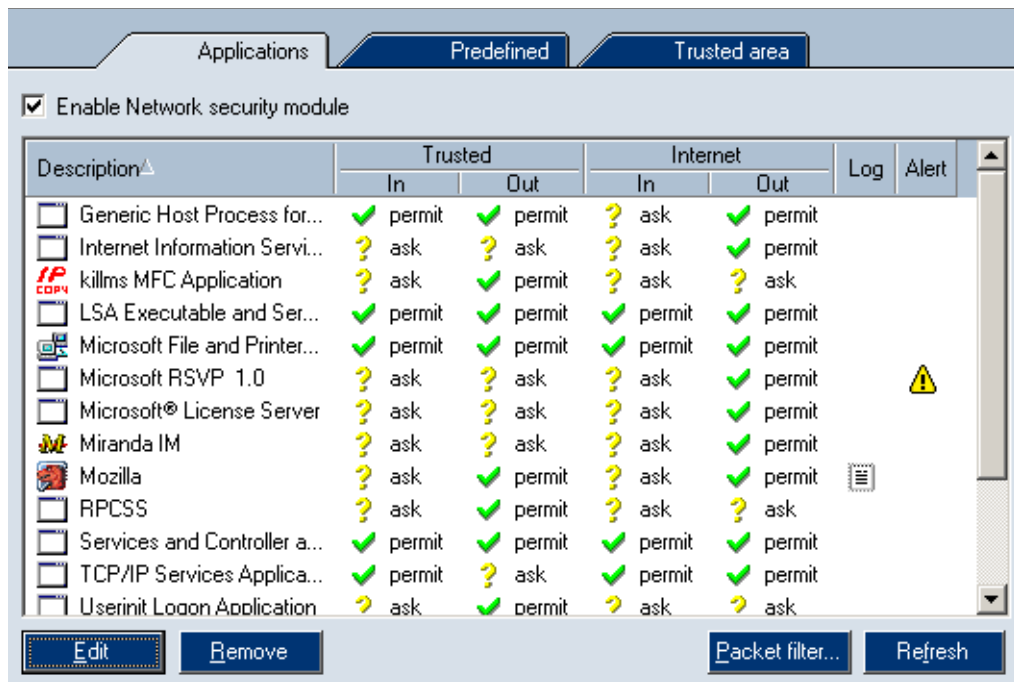
5.1 Pravidla pro aplikace

K zobrazení a úpravě pravidel pro aplikace slouží sekce *Network Security*, záložka *Applications*.

Každé pravidlo sestává z následujících částí:

Description Ikona a popis aplikace. Nemá-li aplikace ikonu, bude použita systémová ikona pro spustitelné soubory. Není-li k dispozici popis aplikace, zobrazí se jméno souboru bez přípony.

Kapitola 5 Pravidla pro síťovou komunikaci



Poznámka: Ikonu a popis aplikace nelze v *Kerio Personal Firewallu* změnit (tyto informace jsou dány tvůrcem konkrétní aplikace).

Trusted, Internet Nastavení chování firewallu při komunikaci dané aplikace s počítačem v důvěryhodné zóně (*Trusted*) a v Internetu v každém směru (*In* — příchozí komunikace; *Out* — odchozí komunikace).


Pro každou zónu a každý směr komunikace lze zvolit jednu z těchto akcí:

- *permit* — povolení komunikace
- *deny* — zákaz komunikace
- *ask* — *Kerio Personal Firewall* se dotáže uživatele, zda chce komunikaci povolit či zakázat. Při zachycení odpovídající komunikace se zobrazí dialog *Connection Alert* (tento dialog je podrobně popsán v kapitole 3.2) a uživatel musí rozhodnout, jak se má firewall zachovat.

Poznámka: V dialogu *Connection Alert* může uživatel pravidlo změnit (zaškrtně-li volbu *Create a rule for this communication...*, pak se akce *Ask* v pravidle změní na akci, kterou uživatel zvolil).

Příklad: Pravidlo pro WWW prohlížeč *Mozilla*

5.1 Pravidla pro aplikace

Description	Trusted		Internet		Log	Alert
	In	Out	In	Out		
 Mozilla	? ask	✓ permit	? ask	✓ permit		

WWW prohlížeč je typická klientská aplikace — navazuje spojení s WWW servery. Odchozí komunikaci (*Out*) tedy můžeme povolit (*Permit*). WWW server ale nikdy ne navazuje spojení zpět na klienta: taková komunikace je podezřelá (může to být pokus o útok). Příchozí komunikaci s aplikací *Mozilla* tedy zakážeme (*Deny*), případně nastavíme akci *Ask*, aby byl uživatel na takovou komunikaci upozorňován.

Log Po zapnutí této volby bude veškerá komunikace vyhovující danému pravidlu zaznamenána do záznamu *Network* (viz kapitola 10.4), a to bez ohledu na nastavenou akci (zaznamenána bude tedy povolená i zakázaná komunikace).

Alert Zapnutím této volby bude při detekci komunikace vyhovující tomuto pravidlu zobrazeno upozornění — okno *Alert* (viz kapitola 3.4). Nezáleží na tom, zda je komunikace povolena či zakázána.

Tuto funkci lze využít např. v případě, kdy zakážeme nežádoucí komunikaci a chceme být informováni o tom, zda a kdy vzdálený počítač pokus o navázání spojení zopakuje.

Tlačítko *Edit* otevírá dialog pro úpravu vybraného pravidla (viz dále). Tlačítko *Remove* odstraní vybrané pravidlo. Tlačítko *Refresh* slouží k obnovení seznamu pravidel (po dobu otevření záložky *Applications* může dojít k interakci firewallu s uživatelem a v důsledku toho k přidání či změně pravidel).

Volby pro pravidla

V poli se seznamem pravidel jsou dostupné následující volby:

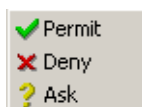
1. Kliknutím pravým tlačítkem myši ve sloupci *Description* se zobrazí kontextové menu s těmito funkcemi:
 - *Edit* — otevření dialogu pro úpravu pravidla (viz níže)
 - *Remove* — odstranění vybraného pravidla
 - *Displayed application name* — volba, jakým způsobem bude zobrazován název aplikace:
 - úplná cesta k souboru (*Full path*)
 - jméno souboru bez cesty (*File name*)
 - popis aplikace (*Description*)

Kapitola 5 Pravidla pro síťovou komunikaci

Volba *Show icon* zapíná/vypíná zobrazování ikony aplikace před jménem souboru nebo popisem aplikace.

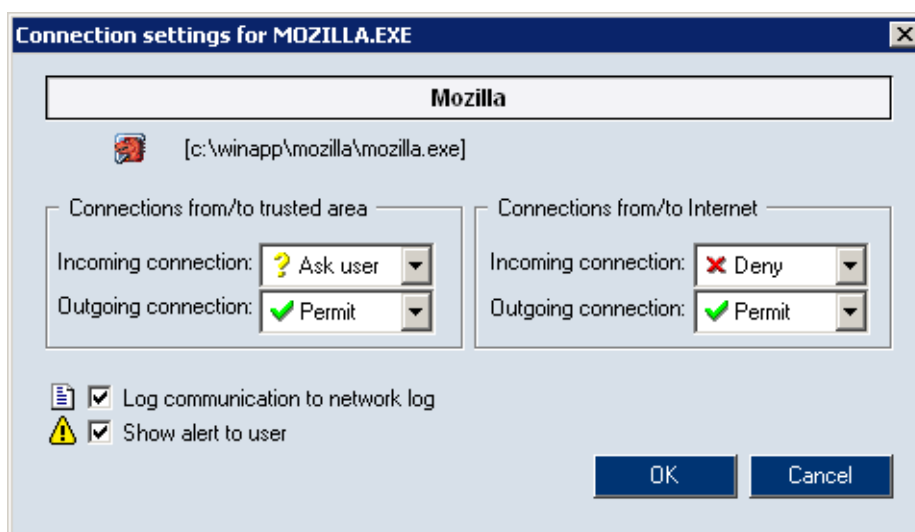
2. Kliknutím myši na akci (ve sloupci *Trusted* nebo *Internet*):

- levým tlačítkem se akce cyklicky přepíná: *Permit* — *Deny* — *Ask*
- pravým tlačítkem se zobrazí kontextové menu, z něhož lze vybrat požadovanou akci.



Dialog pro úpravu pravidla

Stisknutím tlačítka *Edit* nebo volbou *Edit* z kontextového menu se otevře dialog pro úpravu vybraného pravidla. V tomto dialogu lze nastavit akci pro každou zónu a směr komunikace, záznam komunikace odpovídající tomuto pravidlu a zobrazování okna *Alert*.



V horním poli dialogu se zobrazuje popis aplikace a v dalším řádku ikona aplikace a plná cesta k spustitelnému souboru aplikace. Tyto informace nelze měnit.

Střední část dialogu umožňuje nastavení požadovaných akcí pro každou zónu a každý směr komunikace.

Volba *Log communication to network log* zapíná záznam komunikace vyhovující tomuto pravidlu do záznamu *Filter* (viz kapitola 10.4).

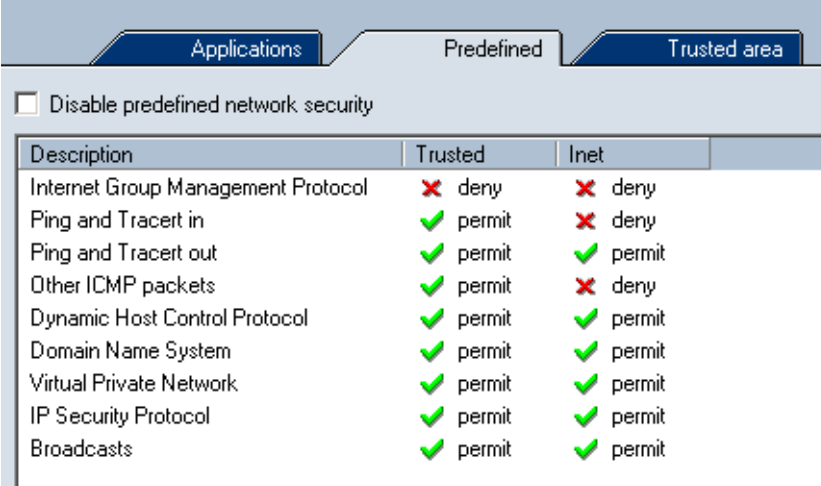
5.2 Předdefinovaná pravidla pro síťovou komunikaci

Volba *Show alert to user* zapíná zobrazování okna *Alert* (viz kapitola 3.4) při zachycení komunikace vyhovující tomuto pravidlu.

5.2 Předdefinovaná pravidla pro síťovou komunikaci

Pro zjednodušení konfigurace obsahuje *Kerio Personal Firewall* sadu předdefinovaných pravidel pro síťovou komunikaci. Tato pravidla nejsou závislá na aplikacích (platí globálně). Uživatel se může rozhodnout, zda předdefinovaná pravidla použije či nikoliv, případně může upravit jejich nastavení.

Předdefinovaná pravidla pro síťovou komunikaci se nacházejí v sekci *Network Security*, záložka *Predefined*.



Description	Trusted	Inet
Internet Group Management Protocol	✗ deny	✗ deny
Ping and Tracert in	✓ permit	✗ deny
Ping and Tracert out	✓ permit	✓ permit
Other ICMP packets	✓ permit	✗ deny
Dynamic Host Control Protocol	✓ permit	✓ permit
Domain Name System	✓ permit	✓ permit
Virtual Private Network	✓ permit	✓ permit
IP Security Protocol	✓ permit	✓ permit
Broadcasts	✓ permit	✓ permit

Pravidla v této záložce nelze přidávat ani odebírat. U každého pravidla lze pouze nastavit akci pro důvěryhodnou zónu (*Trusted*) a Internet. Nastavení akce se provádí kliknutím levým tlačítkem myši na příslušné místo (tj. v řádce vybraného pravidla ve sloupci *Trusted* nebo *Internet*). Opakovaným klikáním se střídavě přepínají akce *Permit* (povolit) a *Deny* (zakázat).

Poznámka: U předdefinovaných pravidel nelze nastavit akci *Ask* (tj. dotázání se uživatele při zachycení odpovídající komunikace — viz kapitoly 5.1 a 3.2).

Volba *Disable predefined network security* zakazuje/povoluje předdefinovaná pravidla pro síťovou komunikaci. Je-li tato volba zaškrtnuta, pak jsou předdefinovaná pravidla ignorována a *Kerio Personal Firewall* pracuje pouze s pravidly pro aplikace (viz kapitola 5.1) a s rozšířeným paketovým filtrem (viz kapitola 5.4).

Tlačítko *Set to defaults* obnovuje výchozí nastavení akcí v předdefinovaných pravidlech.

Kapitola 5 Pravidla pro síťovou komunikaci

Popis předdefinovaných pravidel

Kerio Personal Firewall obsahuje tato předdefinovaná pravidla pro síťovou komunikaci:

Internet Group Management Protocol Protokol *IGMP* se používá k přihlašování a odhlašování do/ze skupiny příjemců multicastových zpráv. Tento protokol lze poměrně snadno zneužít, a proto je ve výchozím nastavení zakázán. Povolte jej pouze v případě, provozujete-li aplikace, které využívají technologie multicast zpráv (typicky přenos zvuku či videa po Internetu).

Ping and Tracert in, Ping and Tracert out Programy *Ping* a *Tracert* (*Traceroute*) slouží ke zjištění odezvy vzdáleného počítače, resp. trasování cesty v síti. K tomuto účelu používají zprávy řídicího protokolu *ICMP* (*Internet Control Message Protocol*).

Případný útočník zpravidla nejprve zkouší, zda vybraná IP adresa „žije“ — tj. zda odpovídá na uvedené řídicí zprávy. Blokováním těchto zpráv se počítač stává „neviditelným“, což může snížit pravděpodobnost útoku.

Ve výchozím nastavení jsou blokovány příchozí *Ping* a *Tracert* zprávy z Internetu. Z důvěryhodné zóny jsou tyto zprávy povoleny (předpokládá se, že např. správce sítě bude programem *Ping* testovat dostupnost dané pracovní stanice).

Odchozí *Ping* a *Tracert* zprávy jsou povoleny pro obě zóny. Tyto nástroje jsou totiž velmi často používány pro ověření funkčnosti síťového připojení či dostupnosti vzdáleného počítače.

Other ICMP packets Pravidlo pro ostatní zprávy řídicího protokolu *ICMP* (např. přesměrování, cíl nedostupný apod.).

Dynamic Host Configuration Protocol *DHCP* slouží k automatickému nastavování parametrů TCP/IP (IP adresa, maska subsítě, výchozí brána atd.).

Upozornění: Zakázání *DHCP* může způsobit nefunkčnost síťového připojení vašeho počítače, pokud jsou parametry TCP/IP konfigurovány tímto protokolem!

Domain Name System *DNS* slouží k převodu jmen počítačů na IP adresy. Aby bylo možné zadávat cílové počítače jmény, musí být povolena komunikace alespoň s jedním DNS serverem.

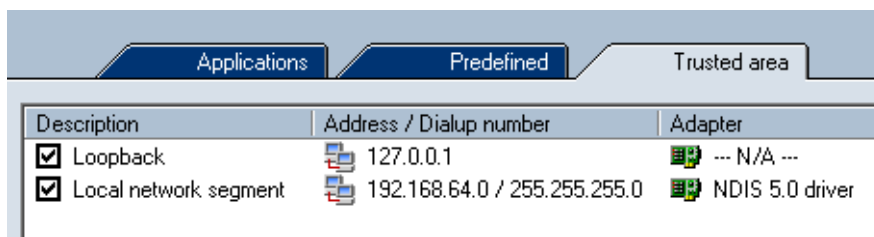
Virtual Private Network Virtuální privátní síť (VPN) je bezpečné propojení dvou lokálních sítí (resp. připojení vzdáleného klienta do lokální sítě) přes Internet šifrovaným kanálem (tzv. tunelem). Pravidlo *Virtual Private Network* kontroluje vytváření VPN protokoly *PPTP* a *IPSec*.

Broadcasts Pravidlo pro pakety se všeobecnou adresou. V zóně *Internet* platí toto pravidlo také pro pakety se skupinovou adresou (multicasts).

5.3 Definice důvěryhodné zóny

Při definici pravidel pro aplikace *Kerio Personal Firewall* rozlišuje dvě skupiny IP adres: důvěryhodnou zónu a Internet. Akce pro příchozí a odchozí komunikaci lze nastavit odděleně pro každou zónu. Důvěryhodná zóna (*Trusted area*) je uživatelsky definovaná skupina IP adres — jaké adresy budou považovány za důvěryhodné, záleží čistě na rozhodnutí uživatele. Všechny IP adresy, které nepatří do důvěryhodné zóny, jsou automaticky zařazeny do zóny *Internet*.

K definici důvěryhodné zóny slouží záložka *Trusted area* v sekci *Network Security*.

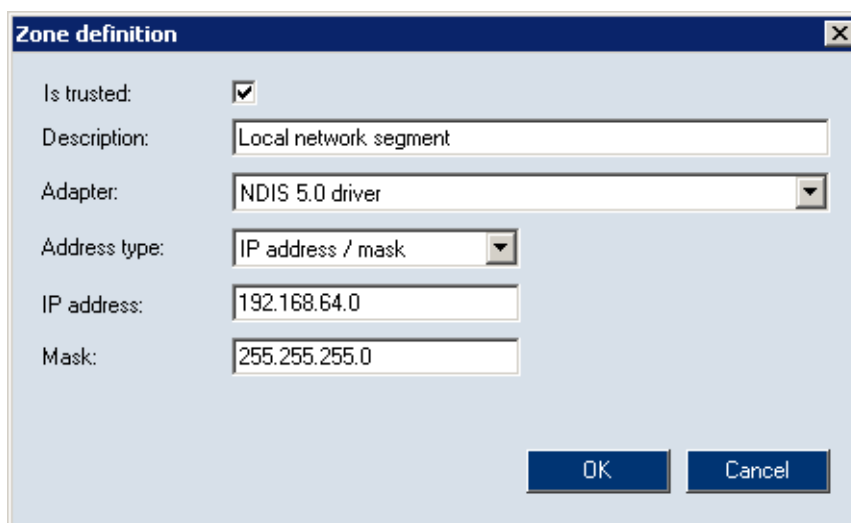


Description	Address / Dialup number	Adapter
<input checked="" type="checkbox"/> Loopback	127.0.0.1	--- N/A ---
<input checked="" type="checkbox"/> Local network segment	192.168.64.0 / 255.255.255.0	NDIS 5.0 driver

Důvěryhodná zóna může obsahovat libovolný počet položek typu IP adresa, rozsah IP adres, subsít' nebo síť připojená k danému rozhraní (podrobnosti viz dále). U každé položky lze volitelně specifikovat rozhraní, na kterém jsou zadané IP adresy povoleny (toto je mj. ochrana proti falšování IP adres).

Důvěryhodná zóna vždy obsahuje jednu předdefinovanou položku *Loopback*, kterou nelze zrušit. Jedná se o lokální zpětnovazební adresu (loopback) — tato adresa je vždy považována za důvěryhodnou.

Tlačítko *Add*, resp. *Edit* otevírá dialog pro přidání, resp. změnu položky důvěryhodné zóny (stejný účinek jako tlačítko *Edit* má také dvojité kliknutí na vybrané položce).



Zone definition

Is trusted:

Description: Local network segment

Adapter: NDIS 5.0 driver

Address type: IP address / mask

IP address: 192.168.64.0

Mask: 255.255.255.0

OK Cancel

Kapitola 5 Pravidla pro síťovou komunikaci

Is trusted Tato volba zařazuje/vyřazuje danou položku do/z důvěryhodné zóny. Je-li volba *Is trusted* vypnuta, uvedené IP adresy (rozsah adres, subsítě atd.) nejsou součástí důvěryhodné zóny (a jsou automaticky zařazeny do zóny *Internet*).

Volbu *Is trusted* lze využít např. pro explicitní specifikaci IP adres, které do důvěryhodné zóny nepatří. *Kerio Personal Firewall* bude znát příslušné rozhraní znát a nebude se dotazovat uživatele při zachycení komunikace přes toto rozhraní (viz kapitola 1.7).

Description Popis položky. Slouží pro zvýšení přehlednosti — doporučujeme uvést stručnou charakteristiku přidávaného rozsahu adres, subsítě atd., případně důvod, proč byly tyto IP adresy do důvěryhodné zóny zařazeny.

Adapter Výběr adaptéru (rozhraní), na kterém jsou zadané IP adresy platné.

Tato volba je také ochranou proti falšování IP adres — je-li paket s důvěryhodnou IP adresou přijat z jiného rozhraní, než ke kterému je daná síť připojena, pak je považován za nedůvěryhodný.

Speciální volba — *Any* — (libovolný adaptér) znamená, že *Kerio Personal Firewall* nebude kontrolovat, z jakého rozhraní byl paket s danou IP adresou přijat.

Address type Typ položky důvěryhodné zóny:

- *Computer* — konkrétní IP adresa jednoho počítače (resp. síťového zařízení)
- *IP address / mask* — subsítě zadaná IP adresou sítě s odpovídající maskou
- *IP address / range* — rozsah IP adres zadaný počáteční a koncovou IP adresou (včetně)
- *All addresses* — libovolná IP adresa

Poznámka: Volbu *All addresses* lze použít pouze ve spojení s konkrétním adaptérem („síť připojená k tomuto rozhraní“). V kombinaci s volbou — *Any* — v položce *Adapter* bychom totiž nastavili, že všechny IP adresy v Internetu patří do důvěryhodné zóny. Toto nastavení nemá smysl a *Kerio Personal Firewall* jej nepovoluje (tlačítko *OK* je v tomto případě neaktivní).

5.4 Rozšířený paketový filtr

Paketový filtr umožňuje definovat detailní pravidlo pro určitou síťovou komunikaci. Kromě lokální aplikace a směru komunikace lze určit také protokol, vzdálené IP adresy, vzdálené a lokální porty a další parametry.

5.4 Rozšířený paketový filtr

Pravidla paketového filtru lze definovat dvěma způsoby:

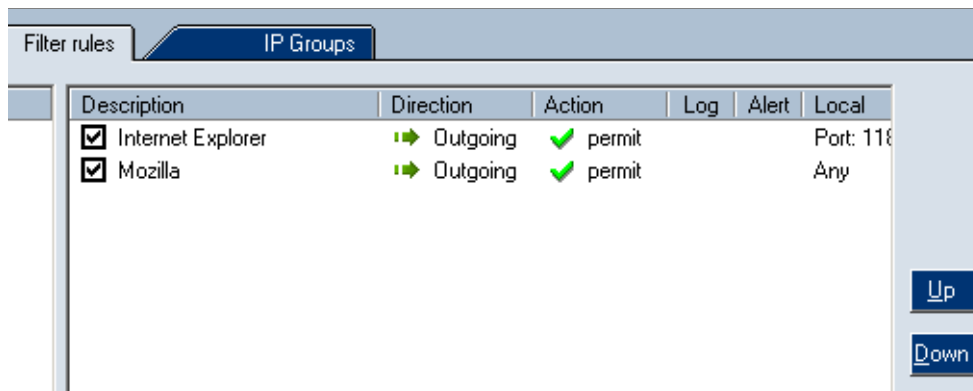
- Ručně — stisknutím tlačítka *Packet Filter...* v sekci *Network Security*, záložka *Applications* se otevře okno *Advanced Packet Filter*, ve kterém lze prohlížet, upravovat a rušit pravidla paketového filtru (podrobnosti viz dále).
- Automaticky, resp. poloautomaticky — při zachycení komunikace, pro kterou nebylo nalezeno odpovídající pravidlo, je zobrazen dialog *Connection Alert* (viz kapitola 3.2); zaškrtnutím volby *Create an advanced filter rule* se namísto standardního pravidla pro aplikace vytvoří pravidlo paketového filtru.

Poznámka: Rozšířený paketový filtr nerozlišuje mezi důvěryhodnou zónou a Internetem (v pravidle je vždy uvedena konkrétní IP adresa, subsíť, skupina IP adres atd.).

Pravidla paketového filtru

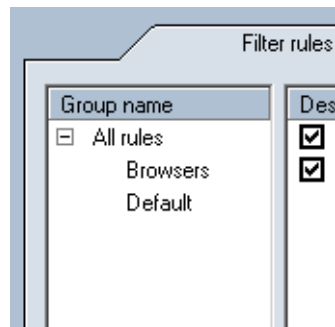
Pravidla rozšířeného paketového filtru se zobrazují v záložce *Filter Rules* okna *Advanced Packet Filter*.

Pravidla tvoří uspořádaný seznam. Při zachycení síťové komunikace se seznam prochází shora dolů a použije se první pravidlo, kterému daná komunikace vyhoví. Tlačítka *Up* a *Down* lze pořadí pravidel v seznamu upravit dle potřeby. Díky těmto vlastnostem je možno vytvářet složitější kombinace filtrovacích pravidel.



Pro zvýšení přehlednosti lze pravidla paketového filtru řadit do skupin. Členství ve skupině nemá žádný vliv na vyhodnocování pravidel — vždy jsou procházena pravidla ve všech skupinách. Skupiny pravidel se zobrazují v levé části záložky *Filter Rules*.

Po kliknutí na jméno skupiny se ve střední části okna zobrazí seznam pravidel patřících do této skupiny.



Následující dvě skupiny jsou předdefinované a nelze je zrušit:

- *All rules* („nadřazená skupina“) — obsahuje všechna pravidla paketového filtru
- *Default* (výchozí skupina) — do této skupiny je automaticky zařazeno každé nově vytvořené pravidlo, pokud uživatel nezvolí jinou skupinu.

Poznámka: Skupiny pravidel nelze explicitně vytvářet a rušit. Skupinu lze vytvořit zadáním názvu nové (dosud neexistující) skupiny při definici pravidla. Zaniká automaticky při odstranění posledního pravidla.

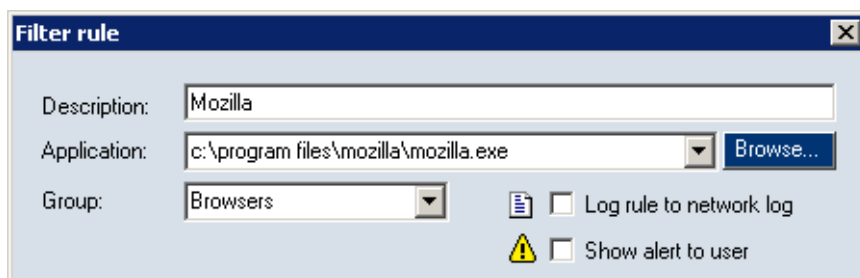
K manipulaci s pravidly paketového filtru slouží tlačítka pod seznamem skupin:

- *Edit* — úprava vybraného pravidla
- *Add* — přidání nového pravidla na konec seznamu
- *Insert* — přidání (vlození) nového pravidla na aktuální pozici (nad označené pravidlo)
- *Remove* — smazání označeného pravidla

Poznámka: Není-li označeno žádné pravidlo, je aktivní pouze tlačítko *Add*.

Vytvoření nebo změna pravidla

Po stisknutí tlačítka *Add*, *Insert* nebo *Edit* se otevře dialog pro definici pravidla paketového filtru. Pravidlo má tyto parametry:



5.4 Rozšířený paketový filtr

Description Název/popis pravidla. Do této položky doporučujeme vyplnit stručný popis pravidla (účel pravidla, název aplikace atd.) — výrazně se tím zlepší přehlednost seznamu pravidel. Do automaticky vytvářených pravidel se jako popis vkládá název lokální aplikace, která se účastní dané komunikace.

Application Lokální aplikace, pro kterou pravidlo platí. Aplikaci lze zadat ručně (jméno spustitelného souboru včetně plné cesty), vybrat ze seznamu (při rozbalení této položky se nabídne seznam aplikací použitých v jiných pravidlech) nebo vyhledat na disku počítače (po stisknutí tlačítka *Browse...* se zobrazí standardní systémový dialog pro otevření souboru).

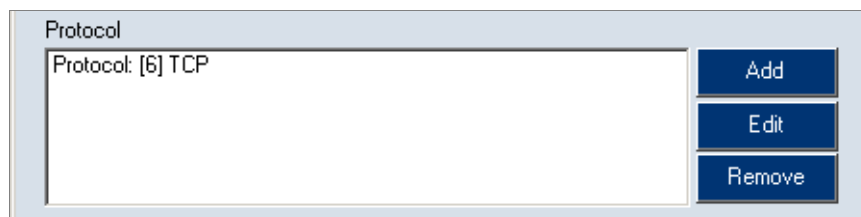
Filtrovací pravidlo může být i obecné, tj. bude platit pro libovolnou aplikaci. Toho dosáhneme výběrem speciální volby *any*, příp. ponecháme pole *Application* prázdné.

Group Skupina pravidel, do které má být pravidlo zařazeno. Zařazení do skupiny nemá žádný vliv na funkci pravidla, slouží pouze pro zpřehlednění seznamu pravidel.

V položce *Group* lze vybrat některou z již existujících skupin nebo zadat název nové skupiny — tím dojde k vytvoření skupiny, do které bude pravidlo zařazeno. Při vytváření nového pravidla je vždy nastavena výchozí skupina *Default*. Totéž platí pro pravidla vytvářená automaticky (viz výše nebo kapitola 3.2).

Log rule to network log Zapnutí/vypnutí záznamu komunikace vyhovující tomuto pravidlu do logu *Network* (viz kapitola 10.4).

Show alert to user Zapnutí/vypnutí zobrazení okna *Alert* (viz kapitola 3.4) při zachycení komunikace vyhovující tomuto pravidlu.



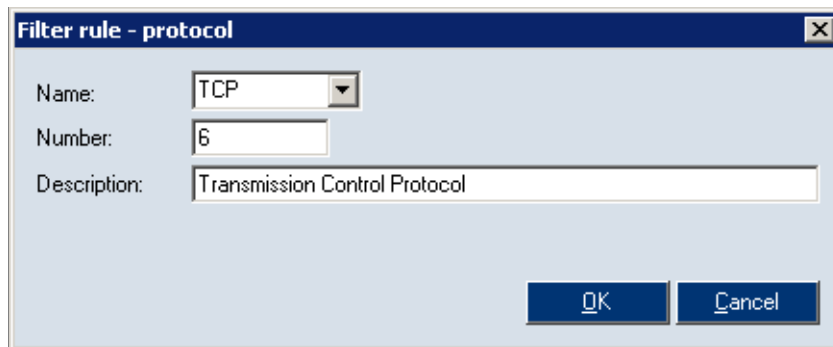
Protocol Nastavení komunikačních protokolů, pro které má pravidlo platit. Typicky je při komunikaci používán jeden protokol (např. TCP nebo UDP), některé aplikace však mohou využívat více protokolů současně (např. TCP a UDP na stejných portech).

Zůstane-li pole *Protocol* prázdné (tj. nezadáme žádný komunikační protokol), bude pravidlo platit pro libovolný komunikační protokol.

Poznámka: Komunikuje-li aplikace protokolem TCP i UDP, přičemž každý protokol používá jiné porty, je třeba v paketovém filtru definovat dvě různá pravidla.

Po stisknutí tlačítka *Add* nebo *Edit* se otevře dialog pro definici protokolu.

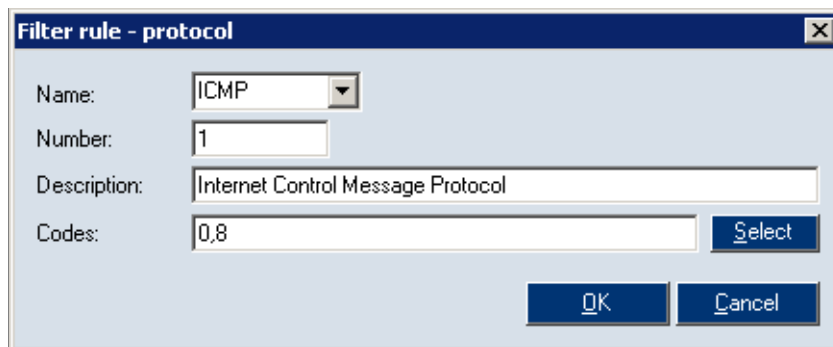
Kapitola 5 Pravidla pro síťovou komunikaci



Protokol je specifikován číslem protokolu v hlavičce IP paketu. Toto číslo lze přímo zadat do položky *Number*. V položce *Name* je možno vybrat některý z předdefinovaných standardních protokolů.

Položka *Description* slouží k zadání popisu protokolu (pro zvýšení přehlednosti). Zobrazuje se pouze v tomto dialogu.

Při výběru protokolu ICMP se v dialogu zobrazí speciální položka *Codes*. V ní lze nastavit typy ICMP zpráv, pro které bude pravidlo platit.

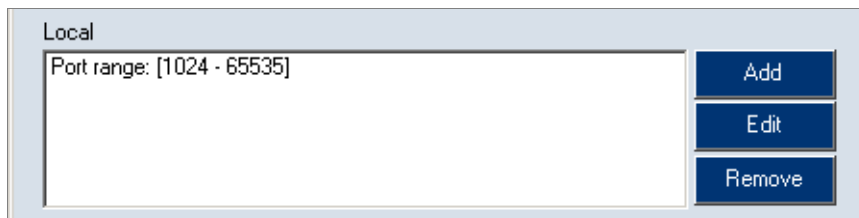


Typy zpráv se zadávají jejich číselnými kódy (jednotlivé kódy musí být odděleny čárkou). Zůstane-li položka *Codes* nevyplněna, bude pravidlo platit pro všechny typy ICMP zpráv.

K snadnému nastavení typů ICMP zpráv slouží speciální dialog, který se zobrazí stisknutím tlačítka *Select*. V tomto dialogu je možné vybrat požadované typy ICMP zpráv. Jejich kódy budou po stisknutí tlačítka *OK* automaticky dosazeny do položky *Codes*.

Local Specifikace lokální strany spojení. *Kerio Personal Firewall* implicitně používá všechny lokální IP adresy včetně zpětnovazebních (loopback). Z tohoto důvodu lze pro lokální stranu spojení specifikovat pouze porty.

5.4 Rozšířený paketový filtr



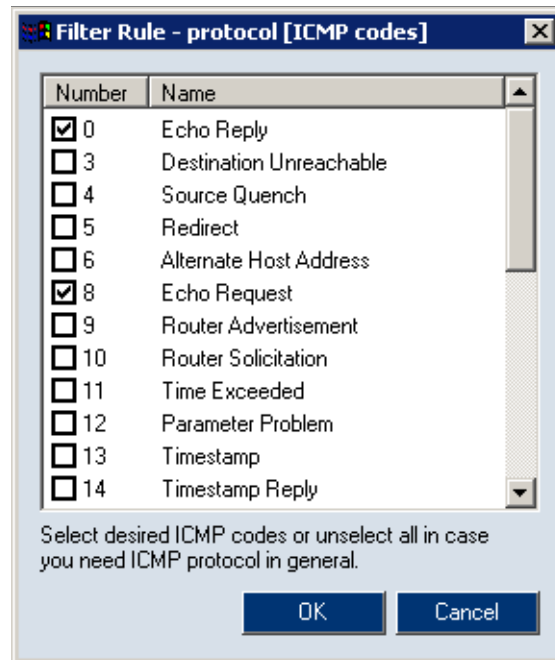
Local

Port range: [1024 - 65535]

Add

Edit

Remove



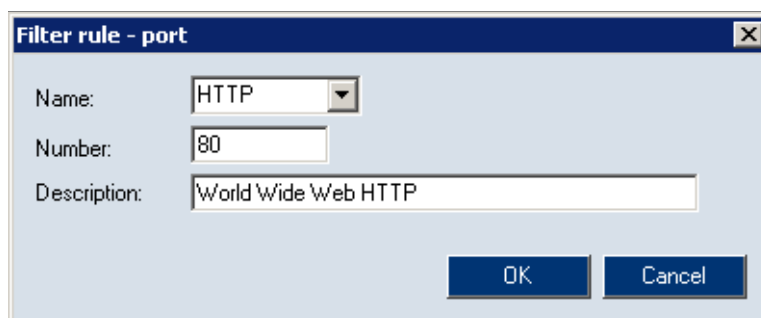
Number	Name
<input checked="" type="checkbox"/>	0 Echo Reply
<input type="checkbox"/>	3 Destination Unreachable
<input type="checkbox"/>	4 Source Quench
<input type="checkbox"/>	5 Redirect
<input type="checkbox"/>	6 Alternate Host Address
<input checked="" type="checkbox"/>	8 Echo Request
<input type="checkbox"/>	9 Router Advertisement
<input type="checkbox"/>	10 Router Solicitation
<input type="checkbox"/>	11 Time Exceeded
<input type="checkbox"/>	12 Parameter Problem
<input type="checkbox"/>	13 Timestamp
<input type="checkbox"/>	14 Timestamp Reply

Select desired ICMP codes or unselect all in case you need ICMP protocol in general.

OK Cancel

Tlačítkem *Add* lze přidat jeden port (*Add port*) nebo rozsah portů (*Add port range*). Jednotlivých portů i rozsahů portů může být zadáno více — takto lze pokrýt libovolnou množinu portů.

Port může být zadán číslem v položce *Number* (platné jsou pouze hodnoty z rozsahu 1-65535) nebo výběrem předdefinované standardní služby v položce *Name*. Položka *Description* slouží k zadání popisu portu, resp. služby (pro zvýšení přehlednosti).



Filter rule - port

Name: HTTP

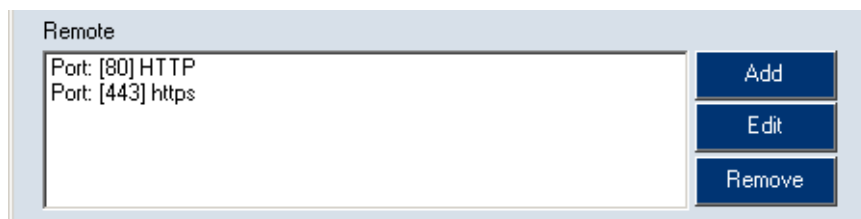
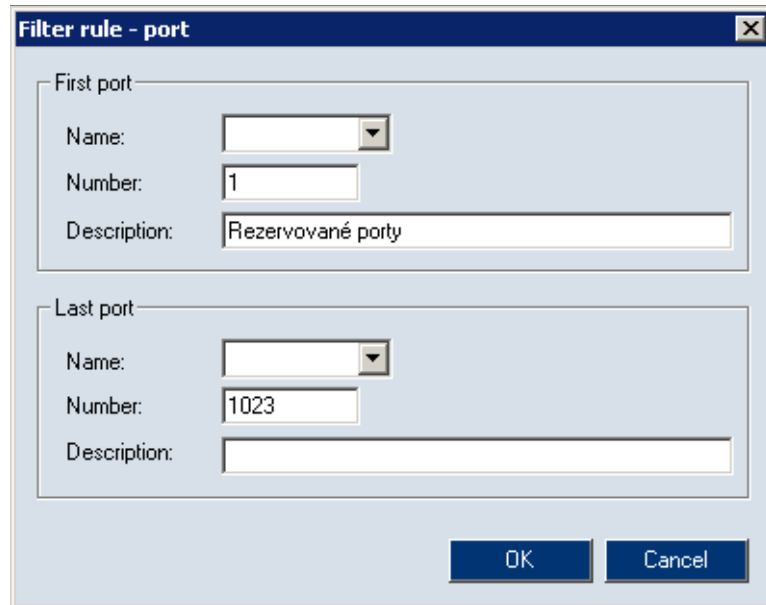
Number: 80

Description: World Wide Web HTTP

OK Cancel

Kapitola 5 Pravidla pro síťovou komunikaci

V případě rozsahu portů dialog obsahuje dvě části: *First port* (počáteční port rozsahu) a *Last port* (koncový port rozsahu).

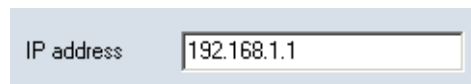


Remote Specifikace vzdálené strany spojení. Dle potřeby je možno zadat IP adresu, port, případně obojí. Pravidlo se pak uplatní, jestliže zachycený paket bude obsahovat některou z IP adres a zároveň některý z portů uvedených v poli *Remote*.

Vzdálený port může být opět zadán jednotlivě (*Add port*) nebo jako rozsah portů (*Add port range*).

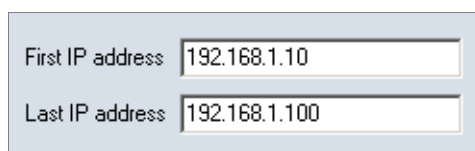
IP adresa může být zadána jako:

- jedna IP adresa (*Add address*)

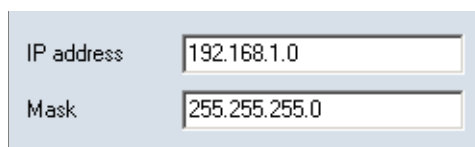


- rozsah IP adres (*Add address range*) — zadáme počáteční a koncovou adresu požadovaného rozsahu

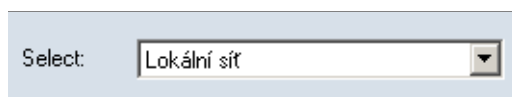
5.4 Rozšířený paketový filtr



- subsítě (*Add address / mask*) — zadáme adresu subsítě a odpovídající masku



- skupina IP adres (*Add IP group*) — v položce *Select* vybereme některou ze skupin IP adres definovaných v záložce *IP Groups*



Jednotlivé možnosti zadání portů a IP adres lze libovolně kombinovat.



Direction Směr komunikace, pro který má pravidlo platit: oba směry (*Both*), příchozí komunikace (*Incoming*) nebo odchozí komunikace (*Outgoing*).

Směrem komunikace je v tomto případě míněn směr navazování spojení (resp. směr prvního paketu, který zahajuje komunikaci).

Action Akce, kterou má *Kerio Personal Firewall* provést při zachycení komunikace odpovídající tomuto pravidlu:

- *Permit* — povolit komunikaci
- *Deny* — zakázat komunikaci

Kapitola 5 Pravidla pro síťovou komunikaci

Logika vytváření pravidel paketového filtru

Při definici filtrovacího pravidla je třeba znát logické vztahy mezi jednotlivými částmi pravidla a položkami v nich obsaženými.

- Vztah mezi poli *Protocol*, *Local* a *Remote* je „a zároveň“. Pravidlu tedy vyhoví komunikace, která splní podmínky ve všech těchto polích.
- Mezi položkami stejného typu (tj. protokoly, IP adresy a porty) v jednom poli platí vztah „nebo“.

Příklad: Pole *Remote* obsahuje dva rozsahy portů: 80–88 a 8000–8080. Podmínka bude splněna, bude-li vzdálený port patřit do jednoho z těchto rozsahů.

- Mezi položkami typu „IP adresa“ a „port“ v poli *Remote* platí vztah „a zároveň“.
- Příklad:* Pole *Remote* obsahuje IP adresu 65 . 131 . 55 . 1 a port 80. Tuto podmínku splní komunikace se vzdáleným počítačem s IP adresou 65 . 131 . 55 . 1 na portu 80.

Poznámky k definici pravidel

Položky *Protocol*, *Local* a *Remote* spolu úzce souvisejí. Při definici filtrovacích pravidel by měl uživatel dodržovat několik základních zásad:

1. Porty mají smysl pouze v případě komunikačních protokolů TCP a UDP. U ostatních protokolů jsou ignorovány.

Platí-li pravidlo pro libovolný protokol (pole *Protocol* je prázdné), pak se porty uplatní v případě, kdy je zachycena komunikace protokolem TCP nebo UDP.

2. Aplikační služba je dána čísly portů a protokoly. V dialogu pro definici filtrovacího pravidla však název služby představuje pouze port — odpovídající protokol je třeba doplnit ručně.

Příklad: Chceme vytvořit pravidlo pro příchozí HTTP komunikaci (např. povolit přístup na WWW server na počítači, který je chráněn *Kerio Personal Firewall*em).

- V sekci *Local* přidáme jeden port (*Add port*), zvolíme službu *HTTP* — tím se nastaví port 80.
 - V sekci *Protocol* musíme nastavit protokol TCP, který služba HTTP používá.
3. Velmi rošířený je model komunikace klient-server, kdy server čeká na známém (dohodnutém) portu na příchozí spojení. Klient při navazování spojení požádá operační systém o přidělení volného lokálního portu (který není předem znám). Z toho vyplývá, že zatímco port serveru musí být znám, port klienta může být (téměř) libovolný.

5.4 Rozšířený paketový filtr

Tyto skutečnosti je třeba brát v úvahu při definici pravidel paketového filtru. Pro ilustraci uvedme dva příklady:

Příklad 1: Chceme povolit přístup k WWW serveru na lokálním počítači z počítače s IP adresou 60.80.100.120. Definujeme pravidlo:

- *Protocol* — [6] TCP (služba HTTP využívá transportní protokol TCP)
- *Local* — Port: [80] HTTP (na lokálním počítači běží WWW server)
- *Remote* — Address: 60.80.100.120 (na vzdáleném počítači bude provozován klient — WWW prohlížeč; port předem neznáme, proto v pravidle uvedeme pouze IP adresu)

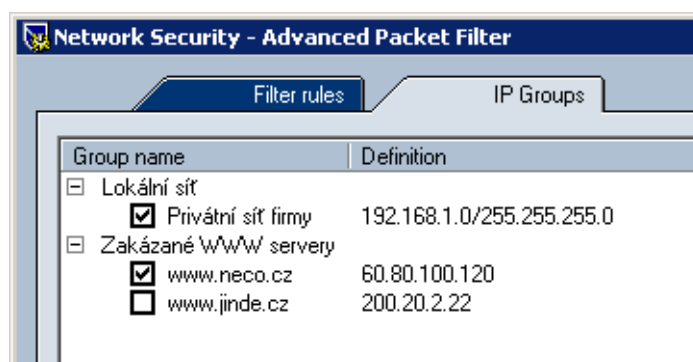
Příklad 2: Z lokálního počítače chceme zakázat přístup k WWW serveru s IP adresou 90.80.70.60. Pravidlo definujeme takto:

- *Protocol* — [6] TCP
- *Local* — toto pole ponecháme nevyplněné (port klienta nelze předem určit)
- *Remote* — Port: [80] HTTP, Address: 90.80.70.60 (specifikujeme vzdálený server)

Skupiny IP adres

Pro snazší definici pravidel paketového filtru je možno vytvářet skupiny IP adres, které pak lze v pravidlech použít v sekci *Remote* dialogu pro editaci pravidel paketového filtru (viz výše).

Skupiny adres se zobrazují a definují v záložce *IP Group* okna *Advanced Packet Filter*.



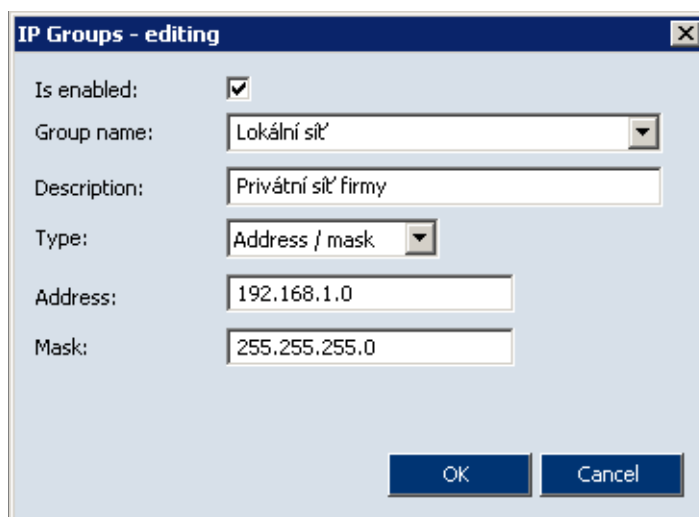
Kapitola 5 Pravidla pro síťovou komunikaci

Okno obsahuje dva sloupce:

- *Group name* — jméno skupiny IP adres, při rozbalení se pod jménem skupiny zobrazí položky obsažené v této skupině
- *Definition* — obsah (definice) jednotlivých položek skupiny

Zaškrtačací pole vedle popisu položky slouží k dočasnému vyřazení položky ze skupiny. Toho lze využívat např. při experimentování a odhalování chyb — položku není třeba odstraňovat a poté znovu přidávat.

Po stisknutí tlačítka *Add* (resp. *Edit*, je-li vybrána nějaká položka) se otevře dialog pro definici skupiny IP adres.



Is enabled Povolení / zakázání položky. Tato volba koresponduje se zaškrtačacím polem vedle názvu položky v záložce *IP Groups* (viz výše). Je-li volba *Is enabled* vypnuta, položka je neaktivní, tzn. není součástí dané skupiny.

Group name Jméno skupiny, do které má být položka zařazena. V tomto poli lze:

- vybrat jméno již definované skupiny — položka bude přidána do této skupiny
- zadat jméno nové (dosud neexistující) skupiny — tím dojde k vytvoření nové skupiny a zařazení položky do této skupiny

Type Typ přidávané položky:

- *Host* — IP adresa jednoho počítače
- *Address range* — rozsah IP adres zadaný počáteční (*First address*) a koncovou (*Last address*) adresou

5.4 Rozšířený paketový filtr

- *Address / mask* — subsítě zadaná adresou sítě s odpovídající maskou
- *Address group* — jiná skupina IP adres (skupiny IP adres lze do sebe libovolně vnořovat).

Kontrola spouštěných aplikací (bezpečnost systému)

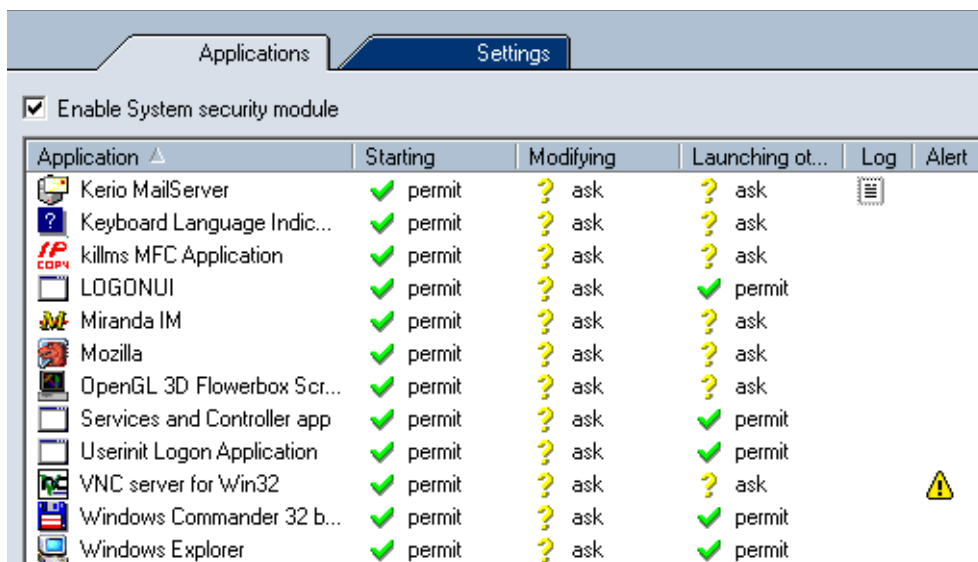
Kerio Personal Firewall má kontrolu nad všemi aplikacemi v operačním systému, bez ohledu na to, zda síťově komunikují či nikoliv. Takto např. dokáže okamžitě odhalit infikaci aplikace novým virem či trojským koněm — narozdíl od antivirového programu, kde vždy existuje určitá prodleva mezi objevením nového viru a příslušnou aktualizací virové databáze.

K nastavení parametrů kontroly aplikací slouží sekce *System Security*.

Volba *Enable System Security module* zapíná/vypíná kontrolu spouštěných aplikací. Je-li tato volba vypnuta, pak *Kerio Personal Firewall* spouštění aplikací nesleduje.

6.1 Pravidla pro aplikace

Záložka *Applications* v sekci *System Security* obsahuje pravidla pro spouštění a záměnu konkrétních aplikací.



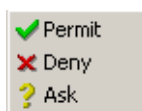
Application	Starting	Modifying	Launching ot...	Log	Alert
Kerio MailServer	✓ permit	? ask	? ask		
Keyboard Language Indic...	✓ permit	? ask	? ask		
killms MFC Application	✓ permit	? ask	? ask		
LOGONUUI	✓ permit	? ask	✓ permit		
Miranda IM	✓ permit	? ask	? ask		
Mozilla	✓ permit	? ask	? ask		
OpenGL 3D Flowerbox Scr...	✓ permit	? ask	? ask		
Services and Controller app	✓ permit	? ask	✓ permit		
Userinit Logon Application	✓ permit	? ask	✓ permit		
VNC server for Win32	✓ permit	? ask	? ask		⚠
Windows Commander 32 b...	✓ permit	? ask	✓ permit		
Windows Explorer	✓ permit	? ask	✓ permit		

Tato pravidla se vytvářejí na základě interakce s uživatelem při spuštění dosud neznámé aplikace. Pravidla nelze vytvářet ručně, lze pouze měnit jejich nastavení nebo je odstranit.

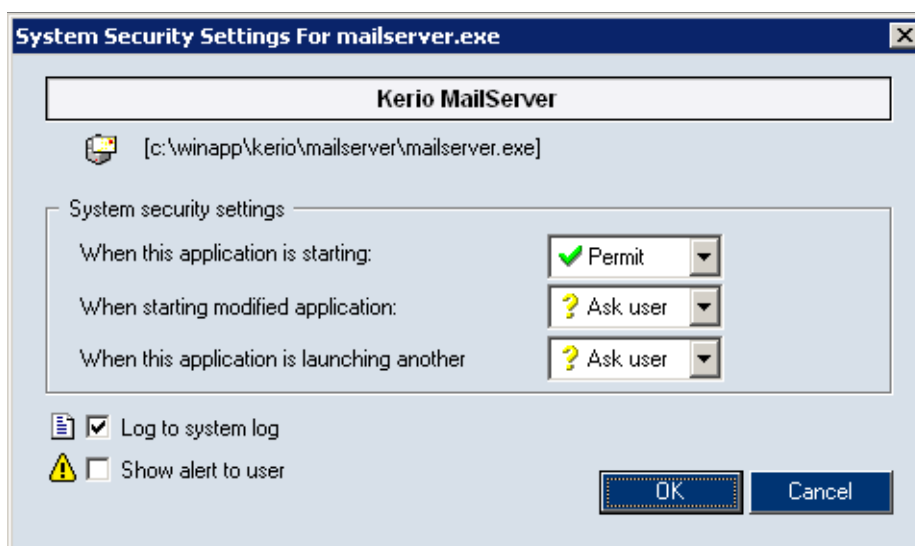
Kapitola 6 Kontrola spouštěných aplikací (bezpečnost systému)

Pro každou aplikaci může uživatel nastavit akci, kterou má firewall provést při spuštění aplikace (*Starting*), při změně spustitelného souboru aplikace (*Modifying*) a při spuštění jiné aplikace touto aplikací (*Launching others*). Akci lze nastavit:

1. přímo v seznamu aplikací — klikáním levým tlačítkem na vybranou akci se cyklicky přepíná: *permit* (povolit), *deny* (zakázat) a *ask* (dotázat se uživatele)
2. v kontextovém menu, které se zobrazí po kliknutí pravým tlačítkem na vybranou akci

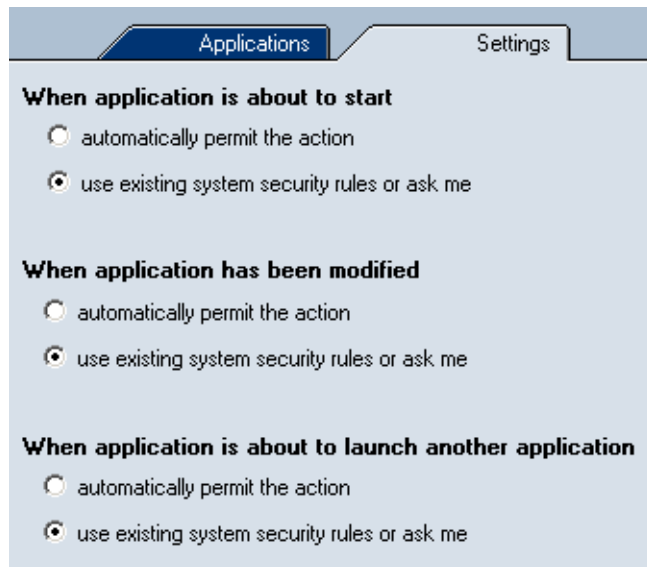


3. v dialogu pro úpravu pravidla. Tento dialog se otevírá tlačítkem *Edit*, příp. volbou *Edit* z kontextového menu vybraného pravidla.



- V záhlaví dialogu je zobrazen popis aplikace, ikona a úplná cesta k spustitelnému souboru aplikace.
- Pole *System security settings* umožňuje nastavení akcí pro výše popsané tři případy.
- Volba *Log to system log* zapíná/vypíná záznam aktivity příslušné aplikace (tj. spuštění, změna spustitelného souboru nebo spuštění jiné aplikace touto aplikací)
- Volba *Show alert to user* zapíná/vypíná zobrazování upozornění — okna *Alert* (viz kapitola 3.4) při aktivitě příslušné aplikace.

6.2 Obecná pravidla



Pravidla v záložce *Settings* určují základní chování firewallu v následujících situacích:

- *When application is about to start* — spuštění aplikace
- *When application has been modified* — změna spustitelného souboru aplikace (při spuštění aplikace se vytvoří kontrolní součet spustitelného souboru a porovná se s kontrolním součtem, který má *Kerio Personal Firewall* uložen ve své databázi)
- *When application is about to launch another application* — spuštění jiné aplikace běžící aplikací

Pro každý z uvedených případů lze nastavit jednu z těchto možností:

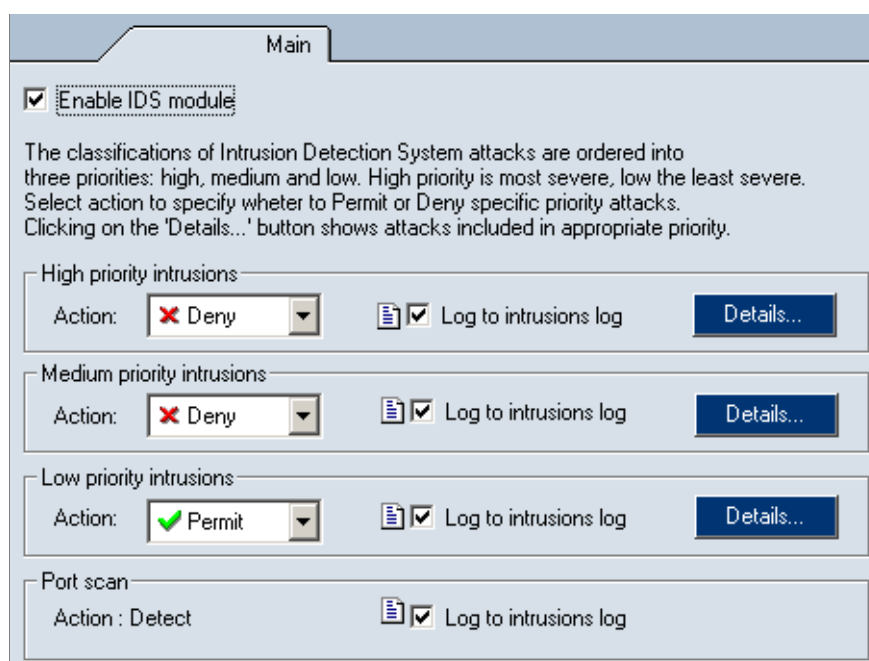
- *automatically permit the action* — automaticky povolit akci. *Kerio Personal Firewall* neblokuje spouštění aplikace, resp. akceptuje záměnu spustitelného souboru)
- *use existing sytem security rules or ask me* — použít pravidlo systémové bezpečnosti pro danou aplikaci (pokud existuje) nebo se dotázat uživatele (viz kapitola 3.3)

Detekce útoků

Kerio Personal Firewall dokáže rozpoznat a blokovat řadu známých typů útoků. K tomuto účelu má vlastní databázi útoků, která je aktualizována s každou novou verzí programu (z tohoto důvodu doporučujeme provádět aktualizaci *Kerio Personal Firewallu* vždy, když se automaticky nabídne).

7.1 Nastavení systému detekce útoků

Parametry systému detekce útoků (*IDS — Intrusion Detection System*) lze nastavit v sekci *Intrusions*.



Volba *Enable IDS module* zapíná/vypíná systém detekce útoků.

Kerio Personal Firewall rozlišuje tři skupiny útoků:

- *High priority intrusions* — kritické útoky — např. poškození operačního systému, pokusy o ovládnutí systému či únik dat

Kapitola 7 Detekce útoků

- *Medium priority intrusions* — útoky, které způsobují např. blokování určitých služeb, nefunkčnost síťového připojení apod.
- *Low priority intrusions* — méně závažné útoky (podezřelé síťové aktivity, chyby v protokolech, neplatný formát dat apod.)

Pro každou z těchto skupin lze odděleně nastavit chování firewallu:

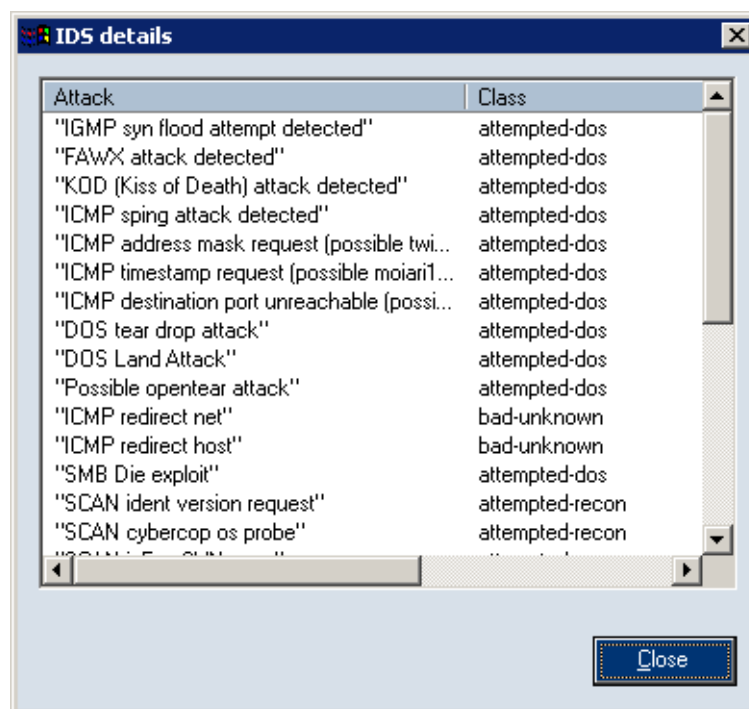
- *Action* — reakce firewallu na útoky z této skupiny (*Permit* — povolit, *Deny* — blokovat).

Obecně je doporučeno blokovat útoky skupin

High priority a *Medium priority* — nepovolujte útoky těchto skupin, pokud si nejste skutečně jisti, co a proč děláte (např. experimentální účely). Útoky skupiny *Low priority* jsou ve výchozím nastavení povoleny — jejich blokování by mohlo způsobovat nefunkčnost určitých služeb.

- *Log to intrusion log* — záznam všech detekovaných útoků z této skupiny do logu *Intrusions* (viz kapitola 10.6).

Tlačítko *Details* zobrazí okno se seznamem útoků v dané skupině.



Okno obsahuje název (popis) útoku (sloupec *Attack*) a třídu útoku (sloupec *Class*). *Kerio Personal Firewall* používá IDS typu *Snort* — podrobné informace naleznete na WWW stránkách <http://www.snort.org/>.

7.1 Nastavení systému detekce útoků

Speciálním případem útoku je tzv. *Port Scanning* (vyhledávání otevřených portů na daném počítači). Z definice Port Scanningu vyplývá, že jej není možné zcela blokovat, pokud má uživatel otevřené nějaké porty (uzavřené porty se automaticky blokují). *Kerio Personal Firewall* jej pouze detekuje — volba *Log to intrusions log* zapíná/vypíná záznam o Port Scanningu do logu *Intrusions*.

Filtrování obsahu WWW stránek

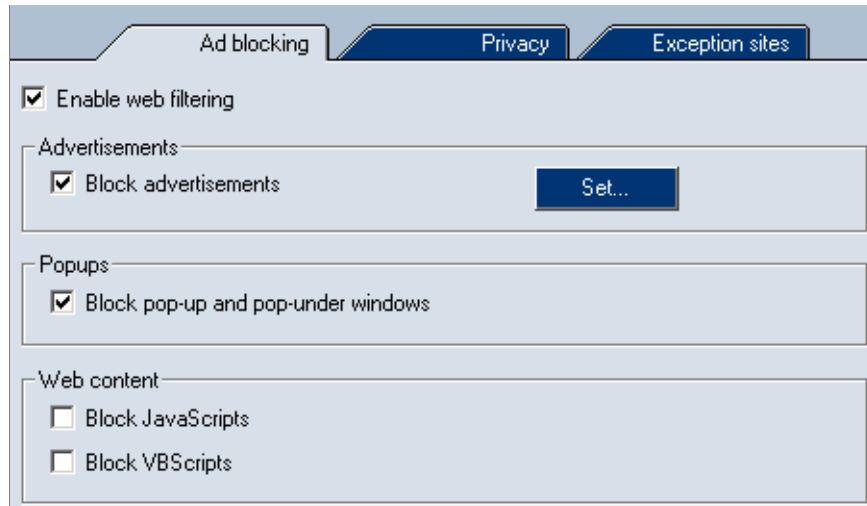
Filtr obsahu WWW stránek v *Kerio Personal Firewallu* má dvě hlavní funkce:

- blokování reklam (tj. bannerů, pop-up oken, skriptů atd.)
- ochrana soukromí (tj. kontrola odesílaných dat a ukládaných cookies)

K nastavení parametrů filtrování obsahu slouží sekce *Web* konfiguračního okna *Kerio Personal Firewallu*.

Volba *Enable web filtering* v záložce *Ad blocking* zapíná/vypíná filtrování obsahu. Je-li tato volba vypnuta, pak neprovádí *Kerio Personal Firewall* kontrolu obsahu WWW stránek.

8.1 Blokování reklam, skriptů a pop-up oken



Kerio Personal Firewall má tyto možnosti filtrování reklam:

Block advertisement Blokování reklam podle definovaných pravidel. Tlačítko

Set otevírá dialog pro definici těchto pravidel (viz dále).

Block pop-up and pop-under windows Zákaz otevírání nevyžádaných oken prohlížeče (*popup* = okno otevřené nad aktuálním oknem, *pop-under* = okno otevřené pod

Kapitola 8 Filtrování obsahu WWW stránek

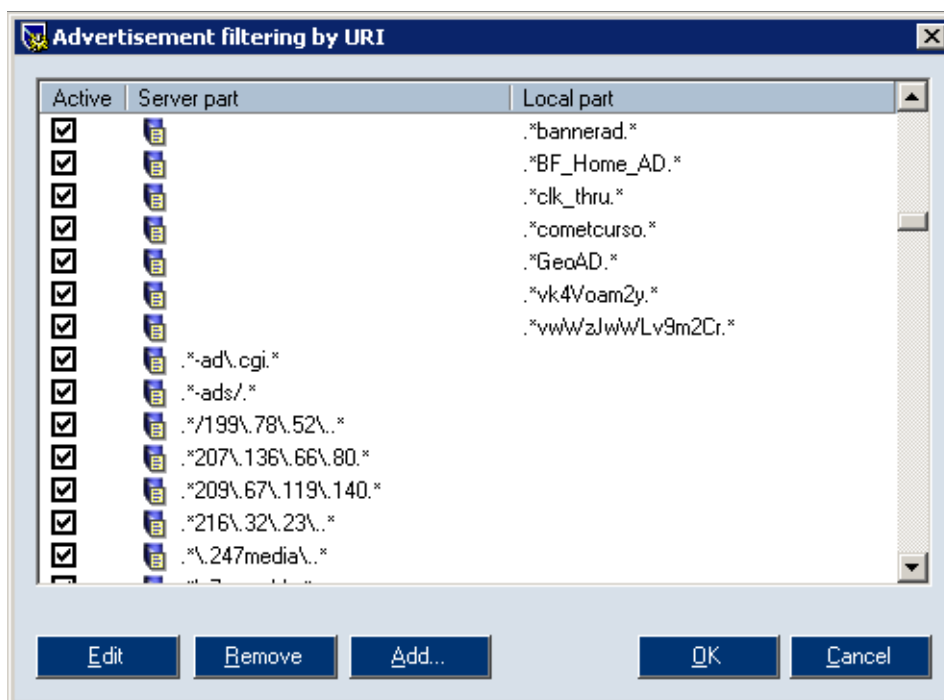
aktuálním oknem — uživatel reklamu spatří po uzavření okna s navštívenou stránkou).

Block JavaScript, Block VBScript Filtrování všech příkazů příslušného skriptovacího jazyka z WWW stránek.

Poznámka: Tyto volby mohou v určitých případech způsobit nesprávné zobrazování některých stránek. Pokud taková situace nastane, je třeba definovat výjimky pro konkrétní stránky v záložce *Exception Sites*, případně volbu *Block pop-up and pop-under windows* nezapínat a filtrovat reklamy jiným způsobem (např. volbou *Block advertisements*).

Pravidla pro filtrování reklam

Tlačítko *Set* otevírá okno s pravidly pro filtrování reklam.



Každé pravidlo je složeno ze dvou částí: *Server part* (jméno nebo IP adresa WWW serveru) a *Local part* (relativní adresa objektu na daném serveru).

Pokud je vyplněna pouze jedna z těchto položek, pak:

- je-li položka *Server Part* prázdná, platí pravidlo pro uvedenou relativní adresu na libovolném serveru
- je-li položka *Local Part* prázdná, pak pravidlo platí pro libovolný objekt na uvedeném serveru (de facto blokování přístupu na tento WWW server)

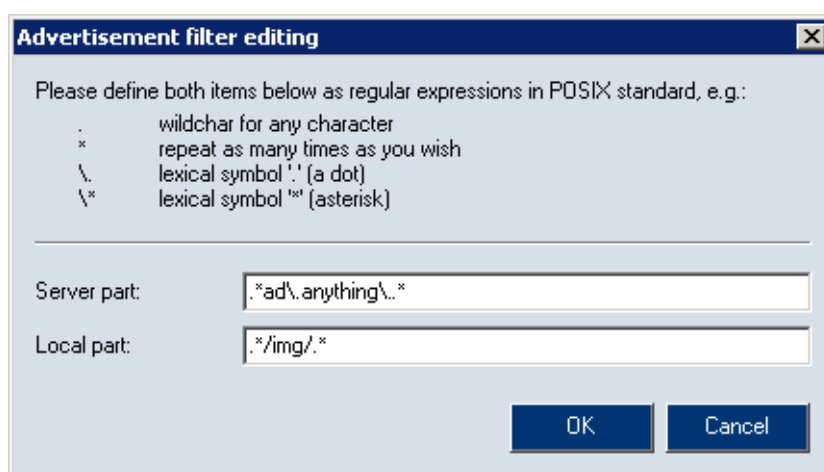
8.1 Blokování reklam, skriptů a pop-up oken

Zaškrtačací pole ve sloupci *Active* zapíná/vypíná příslušné pravidlo. Takto lze pravidlo dočasně „vyřadit“ bez nutnosti jej odstraňovat a poté znovu přidávat.

Tlačítka *Edit*, *Remove* a *Add* slouží pro úpravu či odstranění vybraného pravidla, resp. přidání nového pravidla.

Kerio Personal Firewall má vlastní databázi předdefinovaných pravidel, která jsou označena ikonou. Předdefinovaná pravidla nelze změnit ani odstranit, lze je pouze aktivovat a deaktivovat. Databáze předdefinovaných pravidel je aktualizována při instalaci nové verze *Kerio Personal Firewallu*. Při aktualizaci zůstane zachováno nastavení sloupce *Active* (tzn. při aktualizaci se neaktivují pravidla, která uživatel vypnul).

Tlačítko *Add* nebo *Edit* otevírá dialog pro definici pravidla filtru reklam.



Adresa serveru (*Server part*) i umístění objektu na daném serveru musí být zadáno formou tzv. regulárních výrazů standardu POSIX. Regulární výrazy umožňují popsat libovolný řetězec pomocí speciální symboliky.

Při definici adres WWW serverů a objektů pravděpodobně vystačíme s několika základními symboly:

- . (tečka) — nahrazuje libovolný znak v řetězci.
- * (hvězdička) — znamená libovolný (i nulový) počet opakování předchozího symbolu.
Př.: Výraz *.** představuje libovolný počet znaků.
- \ (zpětné lomítko) — slouží k zadání znaku, který má v regulárním výrazu speciální význam.
Př.: Výraz *\.* představuje znak „tečka“.

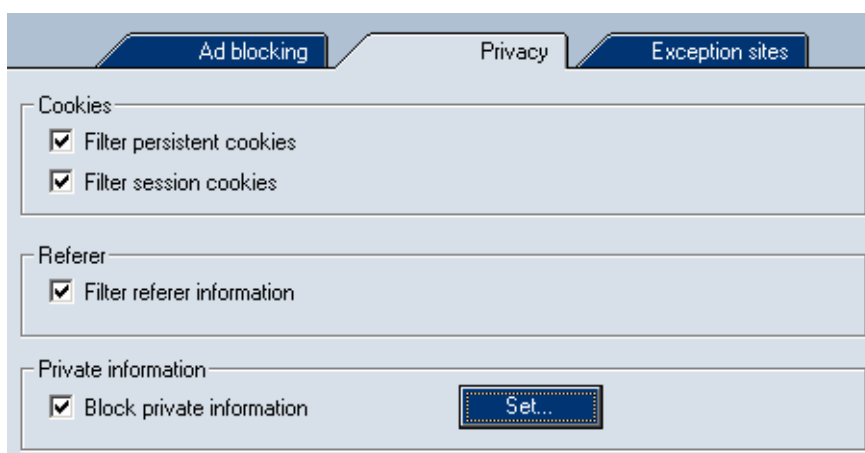
Kapitola 8 Filtrování obsahu WWW stránek

Příklad (viz obrázek):

- Položka *Server Part* obsahuje výraz `.*ad\.anything\.*`.
Tento výraz znamená, že jméno serveru musí obsahovat podřetězec `ad.anything`. — tedy např. `ad.anything.net`, `1ad.anything.com`, `img.ad.anything.cx` apod.
- Položka *Local Part* obsahuje výraz `.*img/.*`.
To znamená, že relativní adresa objektu na serveru musí obsahovat podřetězec `/img/` — tedy např. `/img/banner.gif`, `/data/img/bar.jpg` nebo pouze `/img/`.

Podrobné informace o regulárních výrazech lze nalézt např. na adrese <http://www.gnu.org/software/grep/>.

8.2 Ochrana soukromí uživatele



Záložka *Privacy* obsahuje tyto volby pro ochranu soukromí uživatele:

Filter persistent cookies Filtrování trvale ukládaných cookies.

Tyto cookies obsahují informace, které mohou být odeslány na WWW server při příští návštěvě dané stránky — server tak získá informaci o tom, že uživatel v minulosti tuto stránku již navštívil.

Filter session cookies Filtrování dočasných cookies (ukládáných pouze po dobu jedné relace, tj. do ukončení WWW prohlížeče). Tyto cookies se používají při návratu na příslušnou stránku v rámci této relace — po ukončení relace jsou smazány.

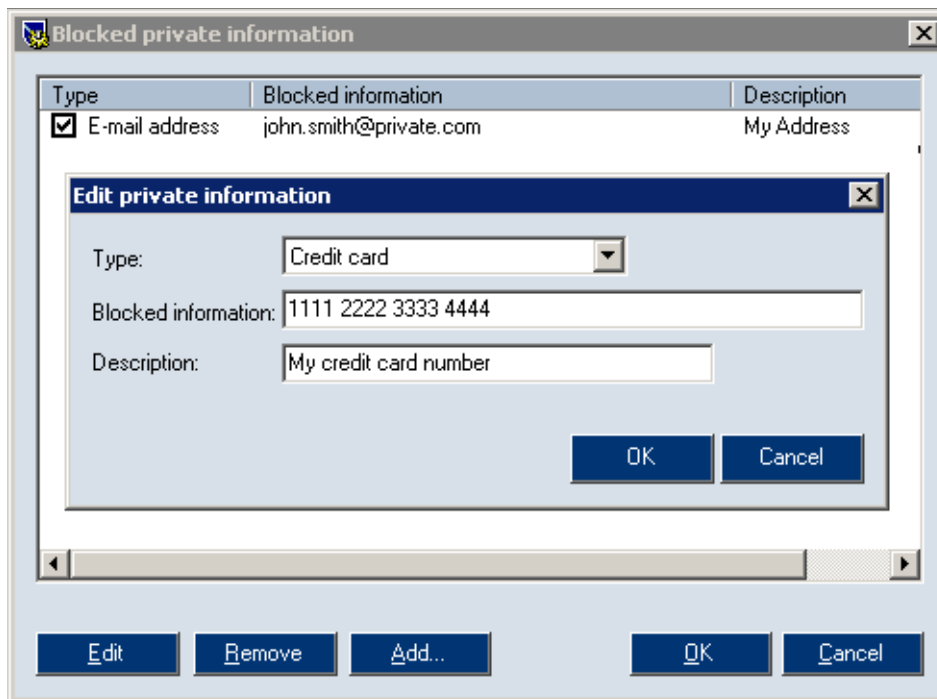
Filter referer information Blokování položky *Referer* v hlavičce protokolu HTTP.

8.3 Výjimky pro jednotlivé WWW servery

Tato položka obsahuje URL stránky, ze které uživatel na danou stránku přišel. Sledováním položky Referer lze mapovat pohyb uživatelů po Internetu.

Block private information Zákaz odesílání definovaných privátních informací protokolem HTTP.

Tlačítko *Set* otevírá okno pro definici privátních informací, jejichž odesílání má *Kerio Personal Firewall* blokovat.



Privátní informace se v *Kerio Personal Firewallu* definuje takto:

- *Type* — výběr typu informace (např. e-mailová adresa, číslo kreditní karty atd.). Tato položka má pouze informativní charakter a nesouvisí s typem pole na WWW stránce.
- *Blocked information* — vlastní informace, tj. řetězec, jehož odeslání bude *Kerio Personal Firewall* blokovat.
- *Description* — popis privátní informace (libovolný text, slouží pro zvýšení přehlednosti).

8.3 Výjimky pro jednotlivé WWW servery

Záložka

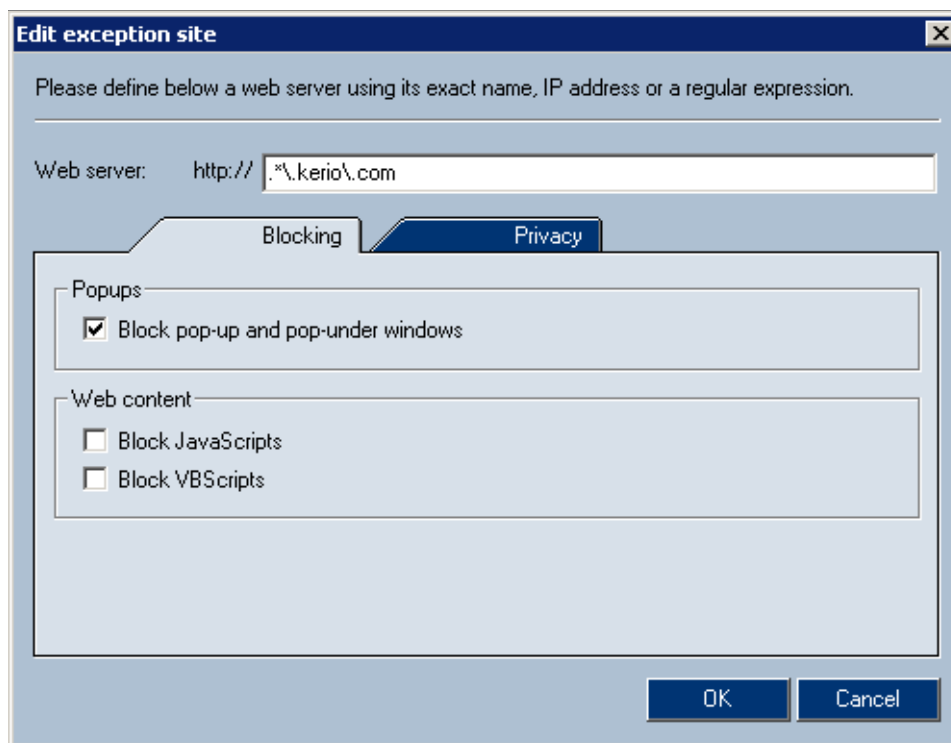
Kapitola 8 Filtrování obsahu WWW stránek

Exception sites umožňuje specifikovat WWW servery, pro které budou nastavena vlastní pravidla filtrování obsahu WWW stránek.



Výjimky pro jednotlivé WWW servery jsou užitečné zejména v případech, kdy obecná pravidla pro obsah WWW stránek (v záložkách *Ad blocking* a *Privacy*) způsobují nefunkčnost určitých stránek (např. otevírání nových oken, přihlašování pomocí e-mailové adresy apod.) nebo jejich úplné zablokování (v důsledku pravidel pro filtrování reklam). Při definici výjimky pro konkrétní server doporučujeme zvážit, zda se jedná o důvěryhodný server a které typy objektů (skripty, cookies, privátní informace) jsou skutečně nutné pro správnou funkci stránek na tomto serveru.

Tlačítko *Add*, resp. *Edit* otevírá dialog pro definici výjimky.



Položka *Web server URL* slouží k zadání jména WWW serveru. Jméno lze zadat formou regulárního výrazu (viz blokování reklam).

8.3 Výjimky pro jednotlivé WWW servery

Zbývající část dialogu tvoří záložky *Blocking* a *Privacy*, které jsou téměř identické s výše popsányými záložkami sekce *Web*. Zde však jednotlivé volby platí pouze pro uvedený WWW server.

Poznámky:

1. Volba *Block private information* není v tomto dialogu doplněna tlačítkem *Set* — privátní informace lze definovat pouze globálně.
2. Záložka *Blocking* neobsahuje volbu *Block advertisements* — blokování reklam lze rovněž nastavit pouze globálně.

Stavové informace

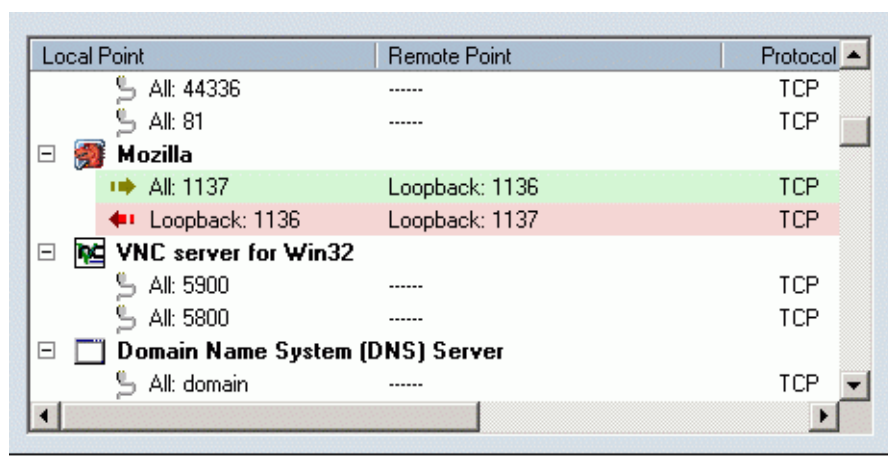
9.1 Přehled spojení a otevřených portů

V sekci *Overview*, záložka *Connections*, se zobrazuje seznam spojení a portů otevřených jednotlivými aplikacemi. Uživatel tak má kompletní přehled, jaké aplikace na jeho počítači sít'ově komunikují nebo čekají na navázání spojení.

Port označujeme jako otevřený, jestliže je v jednom z následujících stavů:

- navázané odchozí spojení (zelené podbarvení)
- navázané příchozí spojení (červené podbarvení)
- čeká na navázání spojení — serverový režim (bez podbarvení)

V záložce *Connections* se zobrazuje seznam aplikací, které mají otevřen alepoň jeden port.



Local Point	Remote Point	Protocol
All: 44336	TCP
All: 81	TCP
Mozilla		
All: 1137	Loopback: 1136	TCP
Loopback: 1136	Loopback: 1137	TCP
VNC server for Win32		
All: 5900	TCP
All: 5800	TCP
Domain Name System (DNS) Server		
All: domain	TCP

Na prvním řádku je vždy uvedena ikona a název (popis) aplikace (nemá-li aplikace ikonu, použije se systémová ikona pro spustitelný soubor; není-li k dispozici popis aplikace, zobrazí se jméno souboru bez přípony). Jednoduchým kliknutím na tlačítko [+] nebo [-] vedle ikony aplikace lze zobrazit, resp. skrýt seznam portů otevřených touto aplikací.

V dalších řádcích jsou pak zobrazena jednotlivá otevřená spojení. Jedná-li se o odchozí spojení, řádek je zvýrazněn světle zelenou barvou; příchozí spojení jsou zvýrazněna světle červenou barvou. Jednotlivé sloupce zobrazují podrobné informace o každém spojení:

Kapitola 9 Stavové informace

Local Point Lokální IP adresa (příp. odpovídající DNS jméno) a port (příp. název služby, jedná-li se o standardní službu).

Namísto DNS jména počítače mohou být uvedena tato speciální jména:

- *All* — port je otevřen na všech lokálních IP adresách (IP adresa 0.0.0.0)
- *Loopback* — lokální zpětnovazební IP adresa (127.0.0.1)

Remote Point IP adresa (resp. DNS jméno) a číslo portu (resp. název služby) vzdáleného počítače. Platí totéž jako pro lokální adresu a port (viz výše).

Protocol Použitý transportní protokol (*TCP* nebo *UDP*, příp. oba).

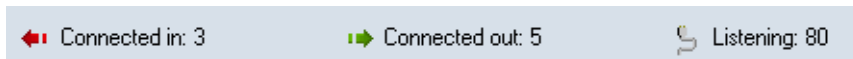
Speed In, Speed Out Aktuální rychlost přijímaných (*In*) a odesílaných (*Out*) dat v rámci daného spojení. Rychlost je uváděna v kilobytech za sekundu (KB/s).

Bytes In, Bytes Out Celkový objem dat přijatých (*In*) a vyslaných (*Out*) v rámci daného spojení.

Poznámka: Jedná-li se o port, na kterém aplikace čeká na příchozí spojení, pak je známa pouze lokální IP adresa, lokální port a protokol.

Otevřené porty a navázaná spojení

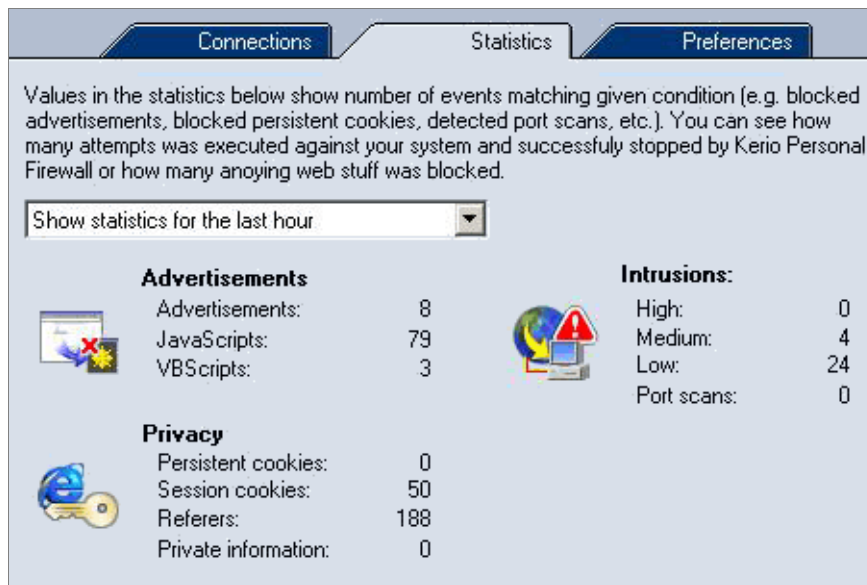
V dolní části záložky *Connections* (stavovém řádku) se zobrazuje aktuální počet spojení a otevřených portů:



- *Connected in* — počet navázaných příchozích spojení
- *Connected out* — počet navázaných odchozích spojení
- *Listening* — počet portů, na kterých aplikace čekají na navázání spojení

9.2 Statistiky

V sekci *Overview / Statistics* lze zobrazit statistiky systému detekce útoků a filtru obsahu WWW stránek za zvolené časové období.



Položka *Show statistics for the last ...* slouží k výběru časového období, za které budou statistiky zobrazovány:

- *hour* — poslední hodina
- *day* — poslední den
- *week* — poslední týden
- *month* — poslední měsíc

Statistiky jsou rozděleny do skupin:

Advertisements Blokování reklam a komponenty WWW stránek:

- *Advertisements* — počet objektů blokových pravidel pro filtrování reklam
- *JavaScripts* — počet filtrovaných skriptů v jazyce *JavaScript*
- *VBScripts* — počet filtrovaných skriptů v jazyce *Visual Basic Script*

Privacy Počet objektů blokových ochrany soukromí uživatele:

- *Persistent cookies* — počet filtrovaných trvalých cookies
- *Session cookies* — počet filtrovaných dočasných cookies

Kapitola 9 Stavové informace

- *Referers* — počet filtrovaných položek *Referer* z hlavičky protokolu HTTP
- *Private information* — počet zablokovaných odesílaných privátních informací

Intrusions Počet detekovaných útoků:

- *High* — kritické útoky
- *Medium* — útoky se střední prioritou (např. blokování služeb)
- *Low* — útoky s nízkou prioritou (např. podezřelé aktivity)
- *Port scans* — zjišťování otevřených portů (*Port Scanning*)

Kapitola 10

Záznamy

Záznamy jsou soubory, které uchovávají historii určitých událostí.

Kerio Personal Firewall má samostatný záznam pro každý modul (*Network*, *System*, *Intrusions* a *Web*).

Dále existují záznamy *Error*, *Warning* a *Debug*, do kterých se zapisují informace vztahující se k běhu programu *Kerio Personal Firewall*. Informace v těchto záznamech mohou být užitečné například při řešení problémů s technickou podporou firmy *Kerio Technologies*.

Soubory záznamů jsou uloženy v podadresáři `logs` adresáře, kde je *Kerio Personal Firewall* nainstalován (typicky `C:\Program Files\Kerio\Personal Firewall 4\logs`). Vlastní soubor záznamu má příponu `.log` (např. `network.log`). Ke každému záznamu přísluší tzv. indexový soubor (pro vyhledávání). Tento soubor má příponu `.idx` (např. `network.log.idx`).

10.1 Prohlížení záznamů

K prohlížení záznamů jednotlivých modulů firewallu a nastavení záznamů slouží sekce *Logs & Alerts*.

Záložka *Logs* obsahuje v dolní části podzáložky se záznamy jednotlivých modulů firewallu. V každé záložce se zobrazuje vždy určitá část příslušného souboru záznamu. Kliknutím na název sloupce lze zobrazenou část záznamu seřadit podle vybraného sloupce.

Z technických důvodů (objem dat) nejsou soubory záznamů načítány celé do paměti. Ze souboru se načte pouze část, která má být zobrazena. Proto při prohlížení záznamů dochází k následujícím jevům:

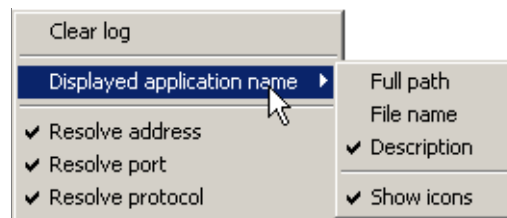
- Zobrazování je při pohybu v záznamu relativně pomalé.
- Při řazení podle vybraného sloupce je seřazena pouze aktuálně zobrazená část záznamu. Po přesunu na jinou část záznamu je třeba zobrazené informace znovu seřadit.

Poznámka: Záznamy *Error*, *Warning* a *Debug* nejsou z uživatelského rozhraní *Kerio Personal Firewall* přístupné — lze je prohlížet pouze jako soubory.

Line	Count	Date	Description
1315	1	06/Aug/2003 16:38:54	"ICMP Echo Reply"
1316	1	06/Aug/2003 16:38:59	"ICMP Echo Reply"
1317	1	06/Aug/2003 16:39:04	"ICMP Echo Reply"
1318	1	06/Aug/2003 16:46:06	"ICMP Echo Reply"
1319	1	06/Aug/2003 16:46:08	"ICMP Echo Reply"
1320	1	06/Aug/2003 16:46:13	"ICMP Echo Reply"
1321	1	06/Aug/2003 16:46:15	"ICMP Echo Reply"
1322	1	06/Aug/2003 16:55:22	"ICMP Destination Unreachable (Und..."
1323	1	06/Aug/2003 16:55:23	"ICMP Destination Unreachable (Und..."
1324	1	06/Aug/2003 16:58:19	"ICMP Echo Reply"
1325	1	06/Aug/2003 16:58:21	"ICMP Echo Reply"
1326	1	06/Aug/2003 16:58:26	"ICMP Echo Reply"
1327	1	06/Aug/2003 16:58:28	"ICMP Echo Reply"
1328	1	06/Aug/2003 17:01:44	"PortScan has been detected"

10.2 Kontextové menu pro záznamy

Při stisknutí pravého tlačítka v záložce se záznamem se zobrazí kontextové menu s volbami pro daný záznam:



Clear log Smazání záznamu. Tato volba smaže veškeré informace z příslušného souboru — smazaný záznam již nelze obnovit.

Displayed application name Způsob zobrazování jmen aplikací:

- *Full path* — úplná cesta ke spustitelnému souboru aplikace
- *File name* — jméno spustitelného souboru aplikace
- *Description* — popis aplikace (je-li k dispozici, jinak je zobrazeno jméno spustitelného souboru bez přípony)

Volba *Show icons* zapíná/vypíná zobrazování ikon aplikací (nemá-li aplikace ikonu, použije se systémová ikona pro spustitelný soubor).

Resolve address Zobrazování jmen počítačů namísto IP adres.

Jména počítačů se zjišťují z DNS (asynchronně). Dokud se nepodaří nalézt odpovídající jméno, je zobrazena IP adresa.

Resolve port Zobrazování jmen služeb namísto čísel portů (pouze pro standardní služby definované v systémovém souboru `services`).

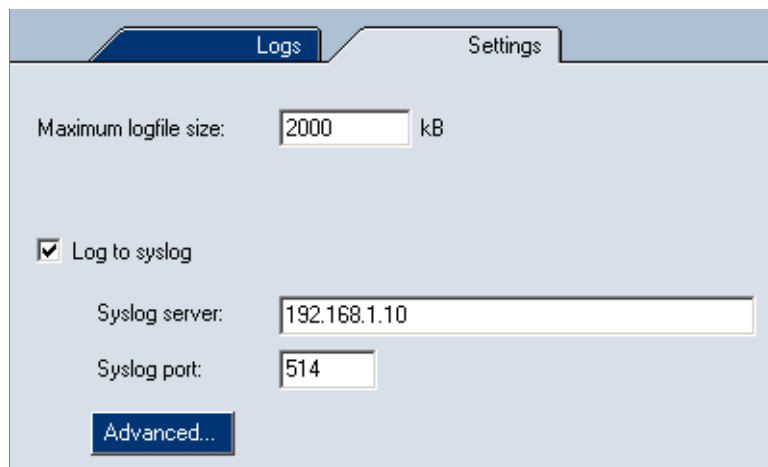
Resolve protocol Zobrazování názvů (zkratk) protokolů namísto čísla protokolu (pouze pro standardní protokoly definované v systémovém souboru `protocols`).

Poznámky:

1. V některých záznamech neobsahuje kontextové menu všechny výše popsané položky — např. v záznamu *System* se nezobrazuje žádná síťová komunikace, a proto zde nejsou volby *Resolve address*, *Resolve port* a *Resolve protocol*.
2. Volby *Displayed application name* a *Resolve address/port/protocol* mají globální platnost — jejich nastavení ovlivňuje všechny záznamy, sekci *Overview / Connections* (viz kapitola 9.1), dialogy *Connection alert* (kap. 3.2) a *Starting / Replacing application* (kap. 3.3) a okno *Alert* (kap. 3.4). Nastavení zobrazování je rovněž popsáno v příslušných kapitolách.

10.3 Volby pro záznamy

V záložce *Settings* sekce *Logs & Alerts* lze nastavit následující parametry a volby pro záznamy (nastavení platí pro všechny záznamy *Kerio Personal Firewall*):



The screenshot shows the 'Settings' window for 'Logs & Alerts'. It features a 'Maximum logfile size' field with the value '2000' and the unit 'kB'. Below this is a checked checkbox for 'Log to syslog'. Underneath, there are two fields: 'Syslog server' with the value '192.168.1.10' and 'Syslog port' with the value '514'. At the bottom left, there is a button labeled 'Advanced...'. The window has two tabs at the top: 'Logs' and 'Settings', with 'Settings' being the active tab.

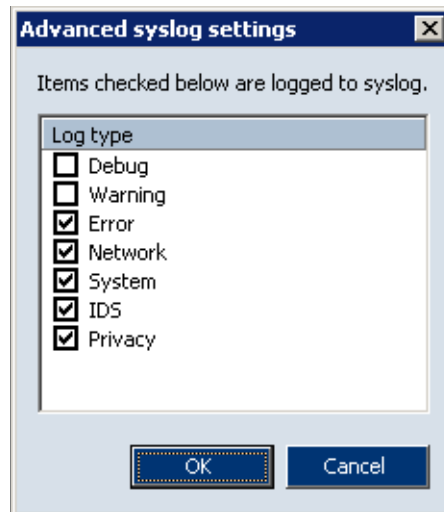
Maximum log file size Maximální velikost souboru záznamu (v kilobytech). Dosáhne-li soubor záznamu této velikosti, bude smazán a zapisován opět od začátku.

Kapitola 10 Záznamy

Log to Syslog Tato volba zapíná/vypíná odesílání vybraných záznamů na *Syslog* server.

Do položky *Syslog server* je třeba zadat jméno nebo IP adresu *Syslog* serveru a do položky *Syslog port* číslo portu, na kterém *Syslog* server běží (standardně 514).

Tlačítko *Advanced...* otevírá dialog pro výběr záznamů *Kerio Personal Firewallu*, které mají být na *Syslog* server odesílány.



10.4 Záznam Network

Do záznamu *Network* se ukládají informace o síťové komunikaci, která vyhověla určitému pravidlu pro aplikaci (viz kapitola 5.1) nebo pravidlu paketového filtru (viz kapitola 5.4). Komunikace se zaznamenává pouze tehdy, pokud je v příslušném pravidle zapnuta volba *Log communication to network log*.

Záznam *Network* obsahuje tyto informace:

Line	Count	Date	Application	Direction	Local...	Remote point	Protoc
0	1	06/Aug/2003 16:55:10	Mozilla	→ out	ferda...	128.242.10...	TCP
1	1	06/Aug/2003 16:55:12	Mozilla	→ out	ferda...	128.242.10...	TCP

- *Line* — číslo řádku záznamu
- *Count* — počet zpráv (opakuje-li se stejná zpráva vícekrát bezprostředně za sebou, uloží se do záznamu pouze jednou a uvede se počet opakování)
- *Date* — datum a čas zápisu zprávy do záznamu
- *Description* — v případě pravidla paketového filtru popis pravidla (obsah položky *Description* příslušného pravidla)

- *Application* — název lokální aplikace (dle volby *Displayed application name*) příslušné k zachycené síťové komunikaci

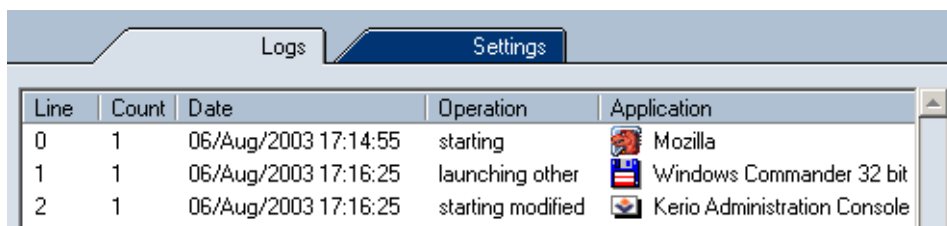
Poznámka: Do souboru záznamu je ukládán jak popis aplikace, tak úplná cesta ke spustitelnému souboru. Proto lze v okně záznamu způsob zobrazení aplikace libovolně přepínat.

- *Direction* — směr navázání spojení (*in* = na lokální počítač, *out* = z lokálního počítače)
- *Local point* — lokální IP adresa (jméno počítače)
- *Remote point* — IP adresa (jméno) vzdáleného počítače
- *Protocol* — použitý komunikační protokol transportní úrovně (TCP, UDP apod.)
- *Action* — akce, která byla provedena:
 - *permitted* — komunikace povolena
 - *denied* — komunikace zakázána
 - *asked* → *permitted* — zobrazen dotaz uživateli (tj. dialog *Connection alert*), uživatel komunikaci povolil
 - *asked* → *denied* — zobrazen dotaz uživateli, uživatel komunikaci zakázal

10.5 Záznam System

Do záznamu *System* se zapisují informace o spouštění aplikací, které vyhovují určitým pravidlům v sekci *System Security / Applications*. Záznam se provádí pouze tehdy, je-li v příslušném pravidle zapnuta volba *Log to system log*.

Záznam *System* obsahuje tyto informace:



Line	Count	Date	Operation	Application
0	1	06/Aug/2003 17:14:55	starting	Mozilla
1	1	06/Aug/2003 17:16:25	launching other	Windows Commander 32 bit
2	1	06/Aug/2003 17:16:25	starting modified	Kerio Administration Console

- *Line* — číslo řádku záznamu
- *Count* — počet identických zpráv

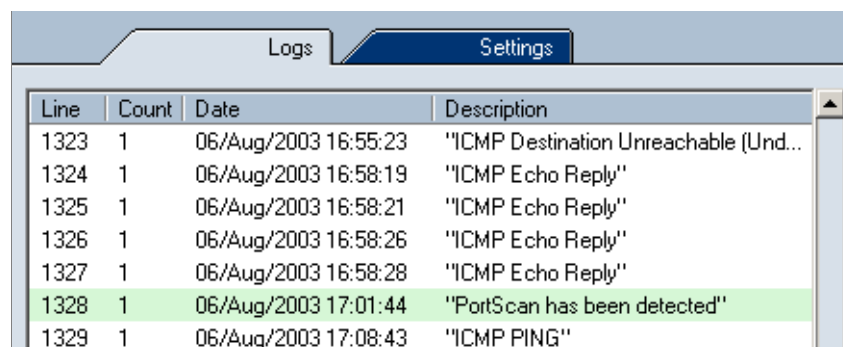
Kapitola 10 Záznamy

- *Date* — datum a čas zápisu zprávy do záznamu
- *Operation* — typ operace:
 - *starting* — spuštění aplikace
 - *starting modified* — změna ve spustitelném souboru aplikace
 - *launching other* — aplikace spouští jinou aplikaci
- *Application* — název aplikace (dle volby *Displayed application name*)
- *Subject* — v případě spuštění jiné aplikace název této aplikace (dle volby *Displayed application name*)
- *Action* — akce, která byla provedena:
 - *permitted* — spuštění aplikace povoleno
 - *denied* — spuštění aplikace zakázáno
 - *asked* → *permitted* — zobrazen dotaz uživateli (tj. dialog *Starting/Replacing/Launching other application*), uživatel spuštění povolil
 - *asked* → *denied* — zobrazen dotaz uživateli, uživatel spuštění zakázal

10.6 Záznam Intrusions

Do záznamu *Intrusions* se zapisují informace o detekovaných útocích. Zaznamenávají jsou útoky těch skupin, u nichž je zapnuta volba *Log to intrusions log* (viz kapitola 7).

Záznam *Intrusions* obsahuje tyto informace:



Line	Count	Date	Description
1323	1	06/Aug/2003 16:55:23	"ICMP Destination Unreachable (Und..."
1324	1	06/Aug/2003 16:58:19	"ICMP Echo Reply"
1325	1	06/Aug/2003 16:58:21	"ICMP Echo Reply"
1326	1	06/Aug/2003 16:58:26	"ICMP Echo Reply"
1327	1	06/Aug/2003 16:58:28	"ICMP Echo Reply"
1328	1	06/Aug/2003 17:01:44	"PortScan has been detected"
1329	1	06/Aug/2003 17:08:43	"ICMP PING"

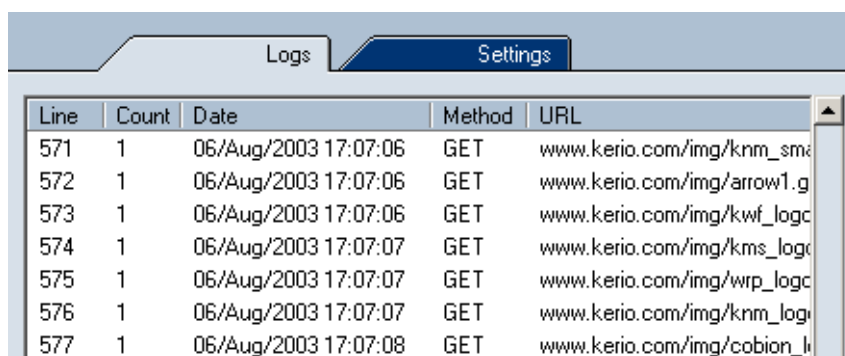
- *Line* — číslo řádku záznamu
- *Count* — počet identických zpráv

- *Date* — datum a čas zápisu zprávy do záznamu
- *Description* — název (popis) zachyceného útoku (viz kapitola 7.1)
- *Direction* — směr útoku (útok může být veden i z lokálního počítače)
- *Remote address* — IP adresa (jméno) vzdáleného počítače (pokud je zjistitelná — útok může být veden z falšované IP adresy)
- *Reference URL* — URL stránky s bližšími informacemi o útoku (jsou-li k dispozici)

10.7 Záznam Web

Do záznamu *Web* se zapisují informace o objektech blokových filtrem obsahu WWW stránek. Tento záznam není konfigurovatelný — je-li modul filtrování obsahu aktivní (viz kapitola 8), zaznamenávají se všechny filtrované objekty.

Záznam *Web* obsahuje tyto informace:



Line	Count	Date	Method	URL
571	1	06/Aug/2003 17:07:06	GET	www.kerio.com/img/knm_sme
572	1	06/Aug/2003 17:07:06	GET	www.kerio.com/img/arrow1.g
573	1	06/Aug/2003 17:07:06	GET	www.kerio.com/img/kwf_logc
574	1	06/Aug/2003 17:07:07	GET	www.kerio.com/img/kms_logc
575	1	06/Aug/2003 17:07:07	GET	www.kerio.com/img/wrp_logc
576	1	06/Aug/2003 17:07:07	GET	www.kerio.com/img/knm_logc
577	1	06/Aug/2003 17:07:08	GET	www.kerio.com/img/cobion_l

- *Line* — číslo řádku záznamu
- *Count* — počet identických zpráv
- *Date* — datum a čas zápisu zprávy do záznamu
- *Method* — použitá metoda protokolu HTTP (*GET* nebo *POST*)
- *URL* — adresa objektu (resp. stránky), kterého se metoda týká
- *Subject* — blokový prvek WWW stránky (*referer*, *cookie* apod.)
- *Value* — hodnota prvku (např. URL v položce *Referer*:, obsah cookie nebo použité pravidlo pro blokování reklam)
- *Action* — akce, která byla provedena (*Removed* = odstraněný prvek z WWW stránky, *Blocked* — blokováno pravidly pro reklamy)

10.8 Záznamy Debug, Error a Warning

Záznam *Debug* obsahuje podrobné informace o běhu programu *Kerio Personal Firewall*.

Do záznamu *Error* se zapisují závažné chyby, které mají zásadní vliv na chod *Kerio Personal Firewallu* (např. nepodaří-li se z nějakého důvodu spustit službu *Personal Firewall Engine*).

Do záznamu *Warning* jsou zapisovány nekritické chyby (např. chyba při zjišťování nové verze programu).

Slovníček pojmů

Aplikační protokol Aplikační protokoly jsou nesený v paketech protokolu TCP, příp. UDP, a slouží přímo k přenosu uživatelských (aplikačních) dat. Existuje mnoho standardních aplikačních protokolů (např. SMTP, POP3, HTTP, FTP apod.), programátor aplikace si však může navrhnout libovolný vlastní (nestandardní) způsob komunikace.

Cookie Textové informace, které server ukládá ke klientovi (WWW prohlížeči). Slouží pro pozdější identifikaci klienta při opětovné návštěvě daného serveru/stránky. Cookies mohou být zneužívány pro sledování, které stránky uživatel navštívil, případně k počítání přístupů.

Firewall Prostředek (zpravidla softwarový produkt) k ochraně před útoky a únikem dat. Existují dva základní typy firewallů:

- síťový firewall — chrání počítače v určité subsíti. Typicky bývá nasazen na bránu (směrovač), který připojuje tuto subsít' do Internetu.
- personální (osobní) firewall — chrání jeden konkrétní počítač (pracovní stanici uživatele). Oproti síťovému firewallu může navíc vztáhnout síťovou komunikaci ke konkrétní aplikaci, měnit své chování na základě interakce s uživatelem atd.

Poznámka: V tomto manuálu je výrazem *firewall* označován produkt *Kerio Personal Firewall*.

ICMP *ICMP* (Internet Control Message Protocol) je protokol pro přenos řídicích zpráv. Těchto zpráv existuje několik typů, např. informace, že cílový počítač je nedostupný, žádost o přesměrování nebo žádost o odezvu (použito v příkazu *PING*).

IP *IP* (Internet Protocol) je protokol, který nese ve své datové části všechny ostatní protokoly. Nejdůležitější informací v jeho hlavičce je zdrojová a cílová IP adresa, tedy kým (jakým počítačem) byl paket vyslán a komu je určen.

Port Nejdůležitější informací v hlavičce TCP a UDP paketu je zdrojový a cílový port. Zatímco IP adresa určuje počítač v Internetu, port určuje aplikaci běžící na tomto počítači. Porty 1-1023 jsou rezervovány pro standardní služby a operační systém, porty 1024-65535 mohou být použity libovolnou aplikací. Při typické komunikaci

Kapitola 11 Slovníček pojmů

klient-server je zpravidla znám cílový port (na něj se navazuje spojení nebo posílá UDP datagram), zdrojový port je naopak přidělován automaticky operačním systémem.

TCP *TCP* (Transmission Control Protocol) slouží pro spolehlivý přenos dat tzv. virtuálním kanálem (spojením). Je používán jako nosný protokol pro většinu aplikačních protokolů, např. SMTP, POP3, HTTP, FTP, Telnet atd.

TCP/IP *TCP/IP* je souhrnné označení pro protokoly používané pro komunikaci v síti Internet. V rámci každého protokolu jsou data dělena na datové jednotky, nazývané pakety. Každý paket se skládá z hlavičky a datové části, přičemž hlavička obsahuje systémové informace (např. zdrojovou a cílovou adresu) a datová část vlastní přenášená data.

Protokolová sada je rozdělena na několik úrovní. Přitom platí, že pakety protokolů nižších úrovní obsahují (zapouzdřují) ve své datové části pakety protokolů vyšších úrovní (např. pakety protokolu TCP jsou nesený v IP paketech).

UDP *UDP* (User Datagram Protocol) je tzv. nespojovaný protokol, tzn. nevytváří žádný kanál a data jsou přenášena v jednotlivých zprávách (tzv. datagramech). UDP nezaručuje spolehlivé doručení dat (datagram se může při přenosu sítě ztratit). Ve srovnání s protokolem TCP má ale mnohem nižší režii (odpadá vytváření a rušení spojení, potvrzování atd.). Protokol UDP se typicky používá např. pro přenos DNS dotazů, zvuku, videa apod.